UNIVERSIDAD AMERICANA
FACULTAD DE INGENIERIA

"Automatización del proceso de transferencia de información entre el Sistema Nacional de Inversión Pública (SNIP) y la Secretaría de la Juventud (SEJUVE) utilizando Redes Privadas Virtuales con Certificados Digitales"

Br. Javier Antonio García Velásquez

Monografía para optar al grado de
INGENIERO EN SISTEMAS

Profesor Tutor
Ing Eden Torres Torres

Managua, Nicaragua, Abril 2004

A mis padres

Javier García y Lesbia Velásquez

Quienes han sido fuente de apoyo

Incondicional en la realización

De este sueño que hoy concluyo

Infinitas Gracias.

AGRADECIMIENTOS

A mis apreciados hermanos: Esnayre Martin, Lissette Mercedes, Jorge Alberto, Eduardo Miguel y Ethel Marina quienes han sido fuentes de inspiración para ser una mejor persona cada día.

A Ericka , cuyo amor y comprensión han sido vitales para seguir luchando en esta vida.

A mi tutor Ing Edén Torres, por haberme brindado el conocimiento, información, críticas y ayuda sin la cual no hubiera sido posible la culminación de este estudio.

A los Ingenieros: José Díaz Chow, Reynaldo Castaño, Trinidad Hernández, Luís Larios, por brindarme su ayuda y conocimiento de manera desinteresada.

A Todas aquellas personas que de manera directa e indirecta tuvieron hicieron posible la culminación de este estudio.

INDICE GENERAL

INTRODUCCION

INTRODUCCION

El presente estudio monográfico, brinda un marco de referencia para la instalación de una Red Privada Virtual (conocida como VPN por sus siglas en inglés) con Certificados Digitales, utilizando Windows 2000 Server como software de implementación. Como parte de los resultados se obtiene una guía de procedimientos que muestra paso a paso, el proceso de instalación de la VPN, así como la instalación de una Infraestructura de Clave Publica (PKI) siendo ésta última, la base para el manejo de certificados digitales que se utilizan como método de autenticación en la VPN.

En Nicaragua, como en el resto del mundo, la necesidad de las empresas y organizaciones de comunicarse tanto dentro como fuera de la misma ha constituido un factor importante para su desarrollo, por lo que la comunicación eficiente se considera como un recurso imprescindible para ofrecer un mejor servicio a usuarios, clientes y proveedores.

La Secretaria de la Juventud (SEJUVE) y el Sistema Nacional de Inversión Publica (SNIP), son instituciones gubernamentales estrechamente ligadas entre si: el SNIP, por ser la institución encargada del seguimiento, evaluación y administración de programas y proyectos de inversión pública que formulan las instituciones que reciben fondos públicos, y la SEJUVE por tener dentro de su mandato institucional, el promover oportunidades y capacidades en la Juventud Nicaragüense a través de programas y proyectos sociales orientados a la juventud, siendo de vital importancia que estas instituciones cuenten con una comunicación ágil, eficiente, veraz y objetiva.

Actualmente ambas instituciones poseen una infraestructura de comunicación que les permite transmitir y compartir información de manera aislada (interna) utilizando Redes de Área Local, pero se dificulta la transferencia de información entre ambas, ocasionando tiempos de respuestas muy grandes en la administración de los proyectos y programas en los cuales están involucradas.

En los últimos años, Nicaragua ha crecido en cuanto a infraestructuras de comunicación se refiere, muchas de ellas subsidiadas por organizaciones internacionales en su afán por ayudar al desarrollo de este país, y otras introducidas por la inversión privada,

todo lo cual ha facilitado que las instituciones gubernamentales y no gubernamentales, sean parte de la "Supercarretera" de la información.

La Instalación de una VPN, utilizando Certificados como mecanismos de autenticación entre las dos instituciones mencionadas, permite que el proceso de transmisión de información sea rápido, seguro y de bajo costo. Decimos de ***bajo costo***, por cuanto solo se requiere de una conexión simple a Internet en vez de equipos dedicados; ***la seguridad*** se obtiene, porque además de que la VPN posee un mecanismo propio de seguridad, se le agrega un nivel más al utilizar Certificados Digitales; y por último ***la rapidez,*** porque al usar ésta tecnología, se logra simular un enlace físico entre las dos instituciones que agiliza la transferencia de información.

Si bien es cierto el uso de una VPN en Nicaragua no es nada nuevo, muchas empresas e instituciones ni siquiera la conocen y las que sí, no han sabido desarrollar su potencial. La tecnología PKI es prácticamente una tecnología nueva, que sólo ha sido utilizada parcialmente en algunos sitios web nacionales en donde se aplica limitadamente a transacciones electrónicas seguras, pero el alcance de una PKI va más allá de eso, puede ser utilizada además, como método de autenticación de equipos y usuarios, y como correo electrónico seguro.

Bajo el contexto antes mencionado, este estudio monográfico brinda la oportunidad a estudiantes y profesionales informáticos para conocer, diseñar e implementar las tecnologías VPN y PKI de manera independiente o en combinación, definiendo de esa manera un punto de partida tanto en el avance de las comunicaciones como en la seguridad de las redes informáticas.

OBJETIVOS

1. General:

Proveer a la Secretaría de la Juventud (SEJUVE) de una solución tecnología de comunicaciones rápida, segura y a bajo costo que le permita automatizar el proceso la transmisión de información concerniente a programas y proyectos con el SNIP.

2. Específicos:

- ✓ Elaborar un análisis Costo-Beneficio de la infraestructura de comunicación que se propone implementar a fin de demostrar su viabilidad técnico-económica.

- ✓ Recomendar una infraestructura básica de telecomunicaciones para lograr la conectividad necesaria para el funcionamiento óptimo de la VPN.

- ✓ Analizar las distintas arquitectas de implementación de VPN con el fin seleccionar la que mejor se adapte a las necesidades de la SEJUVE.

- ✓ Realizar un análisis comparativo entre los protocolos de una VPN a) PPTP (Protocolo para el establecimiento de Túnel Punto a Punto) y b) L2TP (Protocolo para establecimiento de túneles de nivel 2) a fin de seleccionar el que mejor se adapte al propósito de este estudio.

- ✓ Diseñar e implementar una Red Privada Virtual utilizando la arquitectura y el protocolo de establecimiento de túnel que se seleccionaron en los dos objetivos anteriores.

- ✓ Realizar el Análisis, Diseño e Implementación de una Infraestructura de Clave Publica con el propósito de generar, administrar, distribuir y revocar certificados digitales de llave publica.

- ✓ Utilizar Certificados Digitales como método de autenticación en el establecimiento del Túnel de la VPN

I. MARCO TEORICO

I. MARCO TEORICO

A. Redes Privadas Virtuales (VPN)

El auge de las comunicaciones a nivel mundial ha sido tan grande en estos últimos años, que para cualquier empresa e institución es de trascendental importancia contar con una tecnología de comunicación lo suficiente robusta que permita agilizar la transferencia de información de manera segura y a bajo costo entre todas aquellas entidades que necesiten trabajar en conjunto para desempeñar sus actividades y que están separadas geográficamente. Es aquí donde las VPN tienen su mayor utilidad, sin embargo muchas veces los profesionales de la información no se atreven a implementarla por desconocer los conceptos fundamentales, debido a esa situación se presentan los conceptos fundamentales tanto de una VPN como de una PKI para que sirvan de base teórica en la implementación de estas tecnologías.

1. Definición

Una VPN como afirma [BROWN2000, Pág. 5] es: "Un proceso de Comunicación cifrado y encapsulado que transfiere datos desde un punto a otro, de manera segura; la seguridad de los datos se logra gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta e insegura, como INTERNET". Una VPN se puede considerar como la extensión de una red privada en la que se simula un enlace punto a punto seguro con otra red privada distante utilizando la red Internet como enlace.

La simulación del enlace punto a punto se establece al crear un túnel exclusivo en el Internet entre dos puntos(A y B); en este túnel los datos son encapsulados y luego cifrados mediante ciertos mecanismos y solo pueden ser leídos utilizando las claves de descifrado correspondiente.

2. Componentes de una VPN

Una VPN esta conformado por los siguientes componentes:

a) *Servidor VPN*: Es el equipo que acepta una conexión VPN solicitada por un cliente, y generalmente se encuentra en el lugar al cual queremos tener acceso.

b) *Cliente VPN*: Es el equipo que inicia una conexión VPN para el establecimiento del enlace con el servidor VPN.

c) *Túnel*: Es la porción de la conexión en la cual se encapsulan los datos.

d) *Conexión VPN*: Es la porción de la conexión en la cual se encriptan los datos.

e) *Protocolos de Túnel*: Son los protocolos que se utilizan para el establecimiento y manejo de "túneles" en el cual los datos son encapsulados. Entre los protocolos más comunes tenemos: Point to Point Tunneling Protocol (PPTP) y Layer 2 Tunneling Protocol (L2TP).

f) *Datos del Túnel:* Son los datos que son transmitidos en el Túnel.

g) *Red de Tránsito:* Es la Red Publica o compartida que se utiliza para que sirva de enlace en el envío de la información.

En la siguiente ilustración se muestran los componentes de una VPN de manera mas clara.

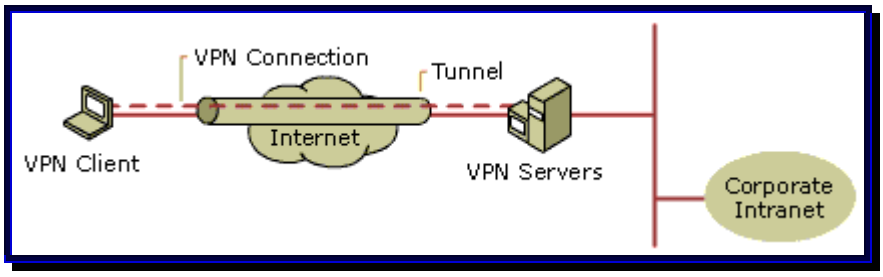


Ilustración I-1: Componentes Principales de una VPN

3. Implementaciones Comunes de una VPN

Una VPN puede ser implementada en cuatro áreas principales:

3.1. Intranet

Este tipo de implementación ocurre cuando se desea enlazar una oficina principal con oficinas sucursales remotas. En este caso los empleados de las oficinas remotas acceden a la red interna de la oficina principal desde el exterior y no desde el interior como comúnmente pasa. En este tipo de VPN sólo participan los empleados de la compañía.

3.2. Acceso Remoto

Este tipo de implementación se da cuando usuarios móviles quieren acceder a la oficina principal de manera remota y utilizando una conexión a Internet para tener acceso a recursos tales como correo, impresión e incluso hasta algunas aplicaciones.

3.3. Extranet

Cuando halla la necesidad de que proveedores y clientes accesen a la red interna de una empresa para obtener información que facilite la toma de decisiones, se utiliza una implementación de VPN Extranet.

3.4. VPN Interna

Algunos Dirigentes de empresas e instituciones consideran que existe información dentro de la misma, que no puede estar accesible a cualquier empleado de la organización, como por ejemplo: información financiera, vacaciones de personal etc. En estos casos se puede utilizar una VPN interna para restringir el acceso solo a aquellas personas autorizadas, asegurándose de esa manera que la información critica con que se cuenta esta protegida y no sea mal utilizada.

4. Arquitecturas de una VPN

Existen tres tipos comunes de arquitectura en una VPN que pueden ser implementados, estos son:

4.1. VPN basada en Software

Esta arquitectura consiste en un software, que implementa tecnología tanto de encriptación como de túneles para poder conectarse a otro computador remoto. El software que se utiliza debe estar instalado tanto en el servidor como en el cliente para que se pueda establecer la conexión.

4.2. VPN basada en Hardware

Esta consiste en dispositivos independientes que al igual que la basada en software utilizan tecnología de VPN como encriptación y creación de túneles para poder establecer el enlace. Estos dispositivos por lo general vienen acompañados de un software para su administración, la cual se puede realizar a través de una interfaz independiente o por medio de un navegador Web.

4.3. VPN basada en Cortafuego o Firewall

Este tipo de arquitectura es la más comúnmente utilizada, se pueden encontrar tanto en hardware como software. Esto no significa que sea la mejor. Su gran auge radica en que la mayoría de las instituciones que tienen una conexión a Internet tienen la necesidad de un mecanismo de protección contra virus, hackers y otros peligros disponibles en la red. Esta necesidad es aprovechada por lo fabricantes de firewall para incorporar dentro de sus sistemas aplicaciones VPN e incluso últimamente hasta PKI.

5. Propiedades de una conexión VPN

La conexión VPN que se utiliza para tener acceso a la información de una empresa u organización remota posee ciertas propiedades de seguridad que garantizan que la información que se envié a través del enlace no sea alterada. Entre estas propiedades podemos mencionar:

5.1. Encapsulación

Una VPN provee un procedimiento para encapsular datos privados con un encabezado de tal manera que permita a los datos atravesar la red abierta, en este caso Internet.

5.2. Autenticación

La autenticación para las VPN se da de dos maneras:

- Autenticación bi-direccional: en la cual el servidor VPN autentica a un cliente que trata de establecer una conexión, de igual forma el cliente autentica al servidor VPN para evitar conectarse a servidores falsos o enmascarados.

- Autenticación e integridad de Datos: Se realiza una comprobación de los datos para verificar de que no hayan sido alterados en su paso por la red abierta, este proceso se lleva a cabo a través de un resumen criptográfico basado en una llave de encriptación conocida únicamente por el origen y el destino.

5.3. Encriptación de Datos

Para asegurar la confidencialidad de la información mediante su paso a través de la red abierta, ésta es cifrada por el origen y descifrada por el destino, de tal manera que aún cuando la información sea interceptada ésta no puede ser descifrada únicamente si se tienen las llaves o claves comunes de encriptación.

5.4. Direcciones y nombres de Servidor para una conexión VPN

Cuando se configura un servidor VPN, se crea una Interface Virtual por medio de la cual serán aceptadas todas las conexiones que se realicen. De igual manera el cliente al conectarse a un servidor VPN crea una interface virtual, que representa el enlace entre el cliente y el servidor, emulando de esa manera el enlace punto a punto. Tanto las interfaces que se crean en el servidor, como las que se crean en el cliente se le asignan direcciones IP. Estas son asignadas de manera manual, o automática utilizando el servicio para asignación de direcciones dinámicas (DHCP - Dynamic Host Configuration Protocol) . Los

clientes VPN obtienen las direcciones de los servidores de nombre de dominio (DNS) y y servidores de nombres de Windows (WINS) de la Intranet a la que se están conectando por medio del servidor VPN.

El tipo de implementación y arquitectura de una VPN que se utilice en una organización depende totalmente, del nivel de seguridad que se requiera así como de los recursos económicos con que se cuenten.

El funcionamiento de una VPN esta basado en la utilización de la tecnología de túneles. Esta tecnología utiliza protocolos como PPTP para crear un canal exclusivo en el enlace de Internet entre dos puntos que los datos puedan ser transmitidos de manera segura y rápida.

6. Tecnología de Túneles

6.1. Entunelamiento

Es el procedimiento o método por medio del cual se trasfieren datos hacia una red, a través de otra red. Los datos (o carga) a ser transferidos o enviados pueden ser los marcos o paquetes de otros protocolo. En vez de enviar los marcos en su estructura original, los protocolos de entunelamiento encapsulan el marco con una cabecera adicional. Esta cabecera adicional provee información sobre enrutamiento de tal manera que la carga encapsulada pueda atravesar una red abierta sin que se pierda.

Los paquetes encapsulados son enrutados entre los puntos extremos de un túnel a través de la red abierta. La ruta sobre la cual viajan los paquetes encapsulados a través de la red abierta es llamada ***Túnel.*** Una vez que los paquetes encapsulados llegan a su destino, los paquetes son desencapsulados y enviados a su destino. El procedimiento de entunelamiento abarca las etapas de encapsulación, transmisión, y desencapsulación de los paquetes.

6.2. Tipos de Túneles

Los túneles pueden ser creados de dos diferentes formas:

- Túneles Voluntarios: Este tipo de túneles son iniciados por el usuario, no necesitan de la intervención de un servidor de acceso a la red NAS (Network Access Server) y requieren que tanto el protocolo de entunelamiento como el software cliente se instalen en la maquina del usuario. En este caso, la computadora del usuario actúa como uno de los puntos finales del túnel y como cliente del túnel. Este tipo de túneles ocurre cuando una estación de trabajo o servidor de enrutamiento utiliza software cliente de túneles para crear una conexión virtual hacia un servidor. La razón para utilizar este tipo de túneles, es que se pueden hacer restricciones de seguridad por el lado el servidor, de tal manera que se asegure un buen uso de los mismos.

- Túneles Compulsivos: Este tipo de túneles utilizan conexiones pre-configuradas a través de dispositivos de inicio. En este caso el NAS del proveedor es el encargado de iniciar la conexión del túnel por el lado del cliente, no requiriéndose de esa manera ninguna configuración por parte del cliente. En este caso el NAS actúa tanto como punto final del túnel, como cliente del túnel. Este tipo de túneles proveen seguridad para conexiones cliente-servidor pero son generalmente usados únicamente cuando los clientes no soportan los voluntarios.

6.3. Protocolos de Entunelamiento

La creación de Túneles en una VPN, se realiza principalmente a través de los protocolos PPTP, L2TP y Internet Protocol Security (IPSEC) cada uno de los cuales presenta ventajas y desventajas. Existe otro protocolo para la creación de túneles, conocido como L2F de la compañía Cisco, pero ha caído en desuso por problemas de desempeño.

El protocolo IPSEC no es meramente un protocolo de túneles, este trabaja en conjunto con L2TP y es el encargado de la parte de encriptación y encapsulación a través de la carga de encapsulación de seguridad (ESP) Encapsulating Security Payload, de ahí que la combinación se conoce como L2TP/IPSEC. La razón por la que no es considerado como protocolo de túnel es que su diseño no fue dirigido para soportar los requerimientos de acceso remoto como son la autenticación de usuarios y la asignación de direcciones, y además porque no tiene soporte para multicast o multiprotocolo ya que esta basado principalmente en el protocolo IP.

Antes de detallar el funcionamiento de los estándares para la creación de túneles es importante referirse al protocolo PPP (Protocolo Punto a Punto) y al Mecanismo de Encapsulación y Enrutamiento Genérico GRE, ya que tanto PPTP y L2TP basan su funcionamiento en base a estos.

6.3.1. Mecanismo de Encapsulación y Enrutamiento Genérico (GRE)

Es el mecanismo que se utiliza para encapsular cualquier protocolo de la capa de red (modelo OSI) en cualquier otro protocolo de la misma capa de red. De manera general un paquete de la capa de red llamada carga de paquete (Payload) es encapsulada en un paquete GRE, al cual también se le incluye información de enrutamiento. El paquete GRE que resulta es encapsulado en otro protocolo de la capa de red llamado protocolo de entrega (Delivery), el cual luego es enviado a su destino.

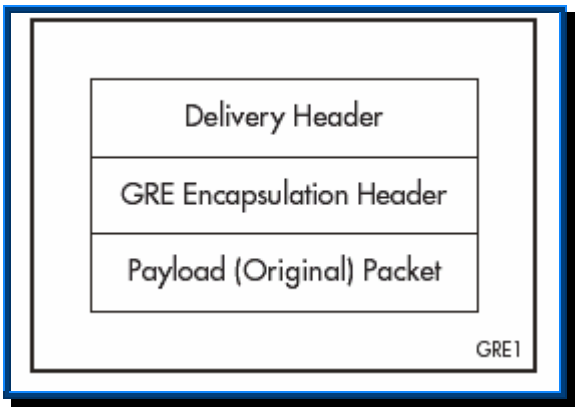


Ilustración I- 2: Formato de un Paquete con encapsulación y enrutamiento genérico VPN.

6.3.2. Protocolo Punto a Punto (PPP)

El protocolo PPP fue diseñado para enviar datos a través de conexiones de línea telefónica o enlaces dedicados punto a punto. PPP encapsula paquetes IP, IPX y NETBEUI en paquetes PPP y luego transmite estos paquetes encapsulados a través del enlace punto a punto. PPP generalmente es utilizado entre un usuario con conexión Dial-Up y un NAS.

Una sesión PPP está regida por 4 fases de negociación:

- Establecimiento del Enlace PPP: PPP utiliza el Protocolo de Control de Enlace (LCP) para establecer, mantener y terminar la conexión física. Durante esta fase los protocolos de autenticación son seleccionados, pero no son implementados hasta la siguiente fase. De igual forma en esta fase se negocia si se utilizará algún tipo de encriptación y compresión aunque su implementación ocurre hasta en la fase cuatro.

- Autenticación de Usuario: En esta fase el cliente o usuario presenta sus credenciales al servidor remoto. PPP incluye los métodos de autenticación: PAP (Password Authentication Protocol); CHAP (Challenge- Handshake Authentication Protocol); MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol); MS-CHAP v2, cada uno de las cuales presenta ventajas y desventajas que serán abordados con posterioridad.

- Control de Llamada de Retorno PPP: Esta fase se incluye en la implementación de PPP de Microsoft. En esta se utiliza el Protocolo de Control de Llamada de Retorno (CBCP) inmediatamente después de la fase de autenticación. El objetivo de esta es que tanto el cliente como el servidor que están estableciendo el enlace se desconectan después de la fase de autenticación y el NAS le regresa la llamada al cliente a un número telefónico específico, para incrementar los niveles de seguridad en la conexión.

- Llamada de Protocolos de Capa de Red: En esta fase, PPP llama a todos los protocolos de control de red (NCPs) que se seleccionaron durante la fase del establecimiento de enlace (Fase 1) con el objetivo de configurar los protocolos usados por el cliente. Por ejemplo, durante esta fase el protocolo IP de Control asigna una dirección dinámicamente al usuario que se conecta por línea telefónica. En la implementación de PPP de Microsoft el Protocolo de Control de Compresión es usado para negociar tanto la compresión de datos como la encriptación de los mismos.

Una vez que se ha llevado a cabo todas estas fases de negociación, PPP empieza a enviar y recibir los datos entre los dos puntos del enlace. Cada paquete de datos transmitidos es empaquetado o encapsulado en una cabecera PPP la cual es removida por

el sistema que la recibe. Si se seleccionó utilizar compresión o encriptación en la fase 1, estas se llevan a cabo antes de la transmisión.

6.3.3. Protocolo de Túneles Punto a Punto (PPTP)

PPTP es un protocolo de capa 2 que encapsula paquetes PPP en datagramas IP para transmitirlos a través de una red abierta como la Internet. PPTP utiliza una conexión TCP conocida como Conexión de Control PPTP para el mantenimiento del Túnel y una versión modificada de GRE para encapsular los paquetes PPP dentro del túnel. La carga del paquete PPP encapsulado puede ser comprimido o cifrado. La siguiente ilustración muestra la estructura de un paquete PPTP.

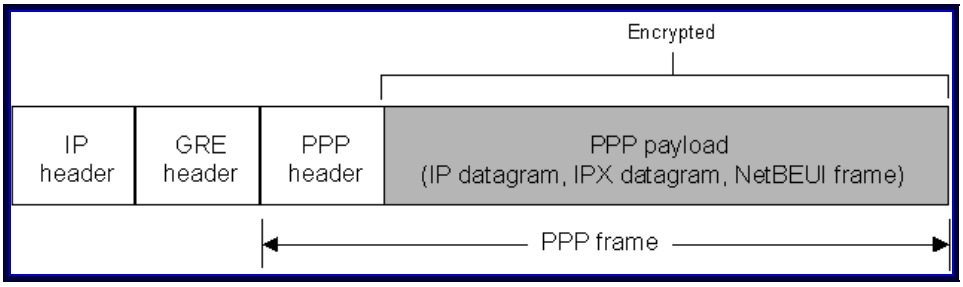


Ilustración I-2: Estructura de un Paquete PPTP conteniendo datos de Usuarios.

La autenticación que ocurre durante la creación de una VPN utilizando PPTP como protocolo de túnel, utiliza los mismos métodos que una conexión PPP tales como EAP, MS-CHAP, PAP y debe utilizar tanto EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) como MS-CHAP para que la carga PPP sea cifrada utilizando el protocolo MPPE (Microsoft Point to Point Encryption), el cual provee solo encriptación de enlace y no encriptación punto a punto. Los servidores PPTP, son servidores VPN con capacidad de manejo de túneles PPTP, que tienen 2 interfaces (Tarjetas de red) una en el Internet y la otra conectada a la red interna.

6.3.4. Protocolo de Túneles de Capa 2 (L2TP)

L2TP es una combinación de las mejores características del protocolo PPTP de Microsoft y L2F (en desuso) de Cisco. L2TP encapsula los paquetes PPP a ser enviados, a

través de redes IP, X.25, Frame Relay y ATM. Cuando se configura para utilizar IP como su transporte de datagramas, puede ser utilizado como un protocolo de túneles a través del Internet.

Cuando se implementa L2TP con redes IP, este utiliza UDP y una serie de mensajes para el mantenimiento del túnel. L2TP también utiliza UDP para enviar paquetes L2TP-PPP encapsulados como los datos dentro del túnel. La carga de los paquetes PPP encapsulados pueden ser encriptados y/o comprimido. A diferencia del PPTP, el cliente L2TP no realiza la negociación de la encriptación utilizando MPPE, mas bien la realiza utilizando ESP de IPSEC. La siguiente ilustración muestra la estructura de un paquete L2TP.

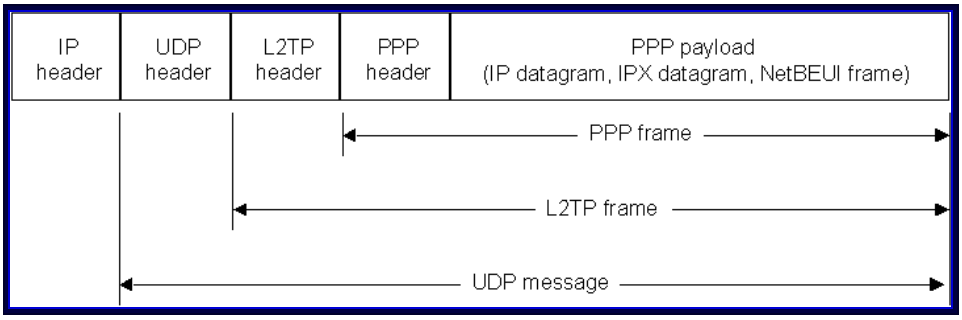


Ilustración I-3: Estructura de un Paquete L2TP conteniendo datos de Usuarios.

L2TP utiliza los mismos mecanismos de autenticación que PPP tales como: EAP, MS-CHAP, CHAP, SPAP, PAP. Los servidores L2TP, son servidores con capacidad de recibir peticiones de marcado, además poseen 2 interfaces (Tarjetas de red), una en el Internet y la otra conectada a la red interna.

6.3.5. Protocolo de Seguridad de Internet IPSEC

IPSEC esta diseñado para proporcionar seguridad básica basada en encriptación para datagramas o paquetes IP. Para brindar esta seguridad IPSEC utiliza dos protocolos de seguridad: El protocolo de Encabezado de Autenticación (AH Authentication Protocol) y el Protocolo de Encapsulamiento de carga de Seguridad (ESP Encapsulating Security Payload).

El protocolo AH de IP proporciona autenticación de origen de datos, integridad sin conexión y un servicio de antirrepetición opcional. El protocolo ESP suministra encriptación y autenticación limitada, en comparación con AH, para datagramas IP. Al igual que AH, ESP proporcionan integridad sin conexión, autenticación de origen de datos y servicio de antirrepetición. Esta característica de los protocolos sin conexión proporciona una barrera para rechazar ataques al servicio.

AH y ESP son los mecanismos que utiliza IPSEC para proporcionar servicios de seguridad a datagramas de IP vinculados a Internet. En general, los dos protocolos de seguridad ofrecen tres clases de servicios:

- Autenticación de Encabezado (AH) y Encapsulamiento de carga (datos transportados por paquetes de IP) para proteger campos e información en "riesgo" en encabezados IP y cargas de paquetes.

- Autenticación y encriptación para protocolos sin conexión de más alto nivel como TCP y UDP. Por lo general, los protocolos sin conexión no proporcionan retroalimentación de "conexión con éxito" entre el emisor y receptor.

- Autoprotección de los agentes de seguridad reales (parámetros), es decir claves de encriptación, que negocian conexiones de IPSEC.

✓ *Asociaciones de Seguridad en IPSEC*

En IPSEC cuando se habilita una conexión mediante AH o ESP, a la conexión resultante se le llama **Asociación de Seguridad (AS)**. Bajo el estándar de IPSEC las AS son tipos específicos de modos de transmisión para paquetes de IP.

A los dos modos de transmisión que utiliza IPSEC para transferencia de seguridad se les llama *modo de transporte* y *modo de túnel.*

✓ *Asociaciones de Seguridad del modo de Transporte en IPSEC*

En modo de transporte, los servicios de seguridad se transmiten directamente al paquete mediante un encabezado AH o ESP. Durante la transmisión, el encabezado de protocolo de seguridad se coloca después del encabezado IP original y de las opciones de

destino, pero antes de la carga o los datos de IP. AH proporciona protección al encabezado IP, las opciones seleccionadas y la carga de IP. ESP solo encapsula la carga con servicios de seguridad.

✓ *Asociaciones de Seguridad del modo de Túnel en IPSEC*

En el caso del modo de túnel, IPSEC anexa un encabezado IP externo. Este suele incluir el destino del procesamiento o puerta de enlace de seguridad de IPSEC. Por lo tanto en el modo túnel, hay dos casos en que ocurre transmisión de punto a punto: entre dos puertas de enlace de seguridad o entre un host (cliente o servidor) y una puerta de enlace de seguridad.

En contraste, IPSEC no agrega un encabezado IP externo en modo de transporte, porque las asociaciones de seguridad a menudo se establecen entre dos anfitriones (para distinguir entre clientes y puertas de enlace de seguridad, los primeros suelen originar o terminar mensajes, mientras que las segundas transfieren mensajes). En la transmisión, el encabezado de protocolo de seguridad se localiza detrás del encabezado IP externo pero antes del encabezado IP original y a la carga de paquete asociada, La protección que proporciona AH es similar a la que proporciona en el modo de transporte. La operación se extiende al encabezado IP externo y a todo el paquete de IP en túnel. ESP, por otro lado, extiende servicios de seguridad solo al paquete de IP en túnel, no al encabezado IP externo.

✓ *Intercambio y Administración de Claves de IPSEC*

El sistema de administración predeterminado de IPSEC para claves de encriptación es ISAKMP/IKE (Internet Security Association and Key Management Protocol Protocol/Internet Key Exchange Protocolo de asociaciones de seguridad de Internet y administración de claves/Intercambio de claves de Internet).

ISAKMP/IKE aseguran que ambos extremos de la VPN utilicen y desplieguen las mismas claves para autenticación y encriptación de paquetes IP. También aseguran que se intercambien las claves a intervalos regulares para reforzar la integridad de transmisiones VPN de manera continua. Con claves de 40 bits o mas débiles, el intercambio de la clave a intervalos regulares es critico, porque si se le brinda el tiempo necesario a un intruso, este puede desencriptar la clave que se esta utilizando.

ISAKMP es un sistema modular, completo, flexible y abierto para aplicación de varios servicios de seguridad originados o desarrollados en las áreas de la organización comercial, federal y de estándares. ISAKMP es el administrador de AS que IPSEC establece para transferir servicios de seguridad. Además es el protocolo que administra el establecimiento y el uso subsiguiente de la clave pública/privada para sesiones seguras de VPN. Específicamente es un marco de referencia que define los procedimientos para:

- Autenticación de una comunicación entre colegas.
- Creación y Administración de AS.
- Transferencia de servicios de seguridad de IP, transporte y capa de aplicación.

✓ *Autenticación de Usuarios con ISAKMP*

La autenticación de usuario es quizás el paso mas importante para establecer un canal de comunicación seguro entre otros nodos de una VPN. Sin la posibilidad de autenticar la entidad en el otro extremo de la conexión, la asociación de seguridad resultante y la clave de sesión para cifrar la sesión actual sigue siendo débil. Para autenticar usuarios, ISAKMP depende de un sistema PKI para generar, verificar, renovar administrar y distribuir certificados digitales, junto con un algoritmo de firma digital, estos certificados establecen las identidades de otras identidades, incluyendo redes, clientes y aplicaciones.

Las firmas digitales son un paso inherente en la utilización de certificados digitales. ISAKMP soporta el proceso de firma digital de RSA o el estándar de firma digital DSS, los cuales se basan en criptografía asimétrica y serán descritos posteriormente. Es importante aclarar que ISAKMP no impone ningún algoritmo de firma digital ni tampoco el servicio para una AC especifica. Lo único que hace es, que una vez que se elige la AC, junto con la información relacionada, este proporciona el medio de mensaje necesario para realizar el intercambio real de autenticación.

✓ *Autenticación de Seguridad e ISAKMP*

Las Asociaciones de Seguridad (AS) son los mecanismos mediante los cuales ISAKMP aplica servicios de seguridad como los servicios de la capa IP. Específicamente define los procedimientos y los formatos de paquetes para establecer, negociar, modificar y

eliminar AS. Una AS es una relación entre dos o más entidades de red, que describe la manera en que se utilizaran los servicios de seguridad para comunicarse de manera segura.

Es decir ISAKMP es utilizado por IPSEC y por otros servicios de seguridad para que negocien AS en su nombre. Los servicios de seguridad de IPSEC se canalizan a través de dos protocolos de seguridad como se mencionó anteriormente, estos son: a) Encabezado de autenticación (AH) y b) Encapsulamiento de carga de Seguridad (ESP).

Al centralizar la administración AS, ISAKMP reduce la cantidad de funcionalidad duplicada dentro de un protocolo de seguridad. Las AS deben soportar diferentes algoritmos de encriptación, mecanismos de autenticación y también algoritmos de generación de claves. Como consecuencia, en ISAKMP las AS están vinculadas con la autenticación y el protocolo de intercambio de claves.

ISAKMP es conocido en la industria por sus servicios de administración de claves, pero dentro de sus propiedades de administración de claves también tenemos otras como, intercambio de claves, autenticación de claves y el secreto perfecto hacia adelante. Se han propuestos dos sistemas de claves para usarse con ISAKMP, estos son: a) IKE (Internet Key Exchange) b) SKIP (Simple Key Management for Internet Protocol).

SKIP es mas adecuado para pequeñas organizaciones, porque es fácil de establecer y no requiere comunicación previa para establecer e intercambiar claves de encriptación. En otras palabras SKIP asume que el esquema de encriptación opera en el otro extremo de la conexión.

IKE por su parte es mas adecuado para organizaciones /empresa mas grandes, porqué ISAKMP permite la negociación de esquemas de encriptación, facilitando mas la conexión con nuevos sitios. IKE recomienda la utilización del protocolo OAKLEY, el cual utiliza un híbrido de la tecnología de cifrado Diffie-Hellman para establecer las claves de sesión. El protocolo Oakley soporta el secreto perfecto, el cual se utiliza con el protocolo ISAKMP para administrar las asociaciones de seguridad.

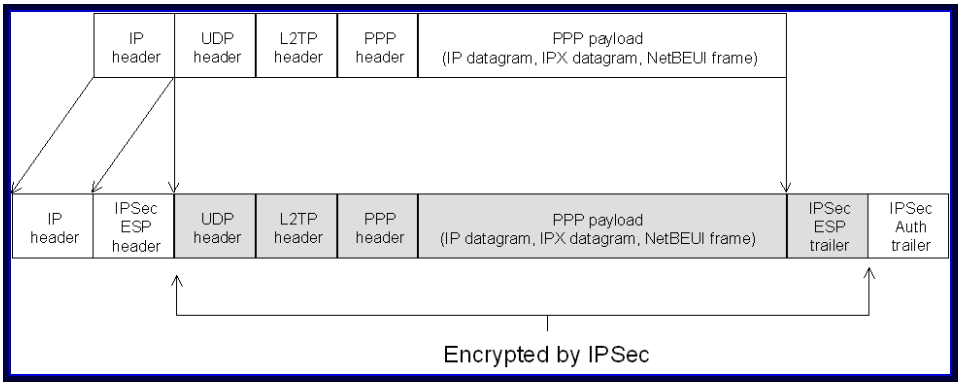


Ilustración I-4: Estructura de un Paquete L2TP cifrado con IPSEC ESP.

B. Certificados Digitales

Como se ha logrado apreciar, las VPN por si sola ofrecen mecanismos de autenticación y encriptación que aseguran que la información que se transmite a través de ella sea confiable. Pero el hecho de utilizar la Internet como medio de enlace, representa una debilidad ya que en algún momento podría verse comprometida. Es por eso que en el presente estudio monográfico se implementa un nivel adicional de seguridad, mediante la utilización de Certificados Digitales. Esta combinación de tecnologías de seguridad y conectividad proporcionan un mecanismo robusto para la transmisión de información en cualquier empresa u organización.

Los Certificados Digitales no son de uso exclusivo de una VPN ya que existen muchas aplicaciones habilitadas para su uso como por ejemplo transacciones electrónicas y correo seguro. La existencia de un Certificado Digital está en dependencia de una arquitectura tecnológica conocida como Infraestructura de Clave Publica PKI la cual a su vez basa su funcionamiento en la Criptografía.

1. Criptografía

Se conoce por criptografía al proceso por medio del cual se trasforma un texto simple o plano en otro llamado texto cifrado que sólo puede ser leído por personas que tengan las credenciales para poder hacerlo. El método o sistema que se utiliza para hacer

esta conversión se denomina algoritmo de encriptación. La ilustración I-5 muestra el proceso básico de encriptación.

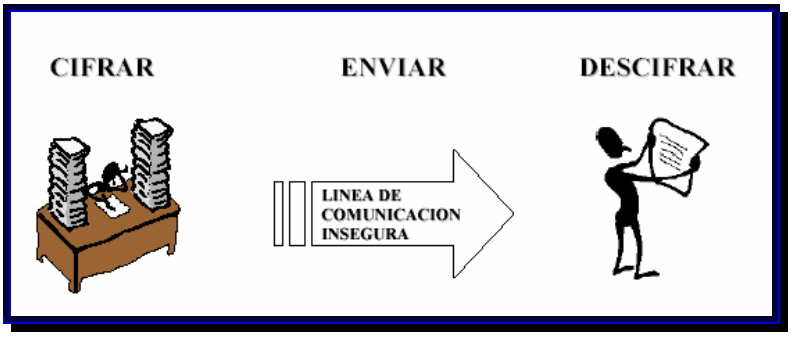


Ilustración I-5: Proceso Básico de Encriptación.

El cifrado de texto es una actividad que ha sido utilizada a lo largo de la historia humana, sobre todo en el campo militar y en aquellas actividades en la que se requiera transmitir información confidencial por medios no seguros.

Mediante la criptografía se pueden resolver los siguientes componentes de seguridad:

- **Confidencialidad**: Esto consiste en asegurar que sólo las personas que tengan autorización puedan acceder a la información cifrada.
- **Integridad**: Consiste en asegurar que la información no haya sido alterada en el transcurso de su transmisión.
- **Autenticación**: Consiste en verificar la identidad de las personas involucradas en la transmisión de texto cifrado.
- **El no rechazo**: Se refiere a que no se pueda negar la autoría de un mensaje enviado.

La criptografía se divide en dos ramas principales: Criptografía de Clave-Llave Privada o Simétrica y Criptografía de Clave-Llave Pública o Asimétrica.

1.1. Criptografía Simétrica

En este tipo de criptografía el emisor utiliza una clave secreta para cifrar el mensaje o información que se quiera enviar, y el receptor debe de conocer la misma clave para poder desencriptarlo. En este tipo de criptografía las claves utilizadas para cifrar la información son de longitud generalmente pequeña lo que facilita su procesamiento.

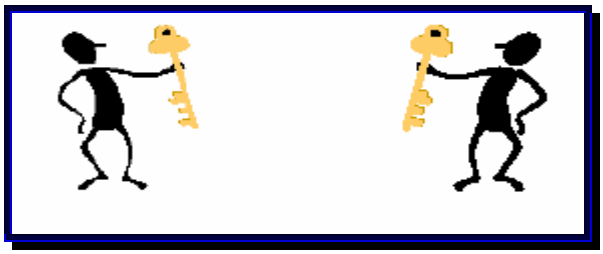


Ilustración I-6: Concepto Básico de la Criptografía Simétrica.

La Criptografía Simétrica esta dividida a su vez en tres familias:

- Criptografía simétrica de bloques (block cipher): la cual se caracteriza por repetir varias operaciones débiles como sustitución, transportación, adición, modular, multiplicación y transformación lineal en un algoritmo mucho mas sólido, en estos se utiliza un tamaño de bloque, un tamaño de clave y un numero de ciclos.

Entre los algoritmos que utilizan este tipo de encriptación encontramos: **DES** un sistema de clave privada de bloques, tanto de cifrado como de descifrado, de 16 ciclos que posee un bloque de entrada con una longitud de 64 bits, produciendo una salida también de 64 bits, con una clave de 56 bits (el octavo bit de cada byte es de paridad), llamada clave externa. Otros algoritmos de bloques incluyen: DES3, TDES, BLOWFISH RC2, RC5.

- Criptografía simétrica de Lluvia (stream cipher): se caracterizan por ser más rápidos que los de bloques y trabajan con bits individuales. Entre los algoritmos tenemos RC4 al cual fue desarrollado por Ron Rivest y utiliza una cifra de flujo de tamaño de clave variable con operaciones algebraicas orientadas a bytes.

- Criptografía simétrica de Resumen (hash functions): Estas transforman un mensaje de longitud variable y generan una cadena de longitud fija, normalmente de 128 bits o más; que se le conoce como valor de transformación de código. Las funciones de

transformación de códigos son de un solo sentido, lo cual significa que son difíciles de invertir o revertir. Cuando un documento experimenta una función de transformación del código este valor se vuelve su "Huella Digital" de tal manera que cuando se habla de firma digital se refiere a la que está en el valor de transformación de código.

Estas funciones de transformación resuelven el problema de la integridad de de la información, al mensaje se le aplica una función hash y se manda junto con el propio mensaje, al recibirlo el receptor aplica la función hash al mensaje y comprueba que sea igual al hash que se envió antes.

Entre los algoritmos hash functions tenemos: Message Digest 2 (MD2), 4 (MD4), 5 (MD5), SHA y SHA-1.

Debido a que, en la Criptografía Simétrica es un requisito que tanto el emisor como el receptor tengan la misma clave secreta, surge el inconveniente para ponerse de acuerdo en la clave que van a utilizar estando en una red abierta donde esta puede ser interceptada, la Criptografía Asimétrica se encarga de resolver este inconveniente.

1.2. Criptografía Asimétrica

En este tipo de criptografía, tanto el emisor como el receptor poseen un par de claves, una para cifrar los datos llamada clave Pública y otra para desencriptar denominada clave Privada. El nacimiento de esta criptografía surge como resultado de la búsqueda de una solución para asegurar el intercambio de las claves simétricas. Es debido a eso, que las dos aplicaciones principales para la utilización de este tipo de criptografía son: Intercambio de las Claves Simétricas y Firma Digital.

La criptografía asimétrica se divide en tres familias según el problema matemático sobre el cual basan su seguridad. La primera basa su seguridad en el Problema de Factorización Entera (PFE), entre los algoritmos de esta familia tenemos: RSA y Rawin Williams (RW). La segunda basa su seguridad en el Problema del Logaritmo Discreto (PLD), a esta familia pertenece el sistema Deffie Hellman (DH) de intercambio de Claves y el sistema DSA de firma Digital. La tercera familia basa su seguridad en el Problema del

Logaritmo Discreto Elíptico (PLDE) en el cual existen varios algoritmos como DHE, DSAE.

El proceso que se lleva a cabo en la Criptografía Asimétrica es el siguiente:

- El emisor encripta los datos o texto original con una llave simétrica generada aleatoriamente.

- El emisor encripta la llave privada, utilizando la llave pública del receptor y se envía tanto los datos encriptados como la llave cifrada.

- Una vez que el receptor los recibe utiliza su llave privada para desencriptar la llave privada del emisor. Debido a que el emisor cifró su llave simétrica utilizando la llave publica del receptor, solo este que posee la llave simétrica complementaria puede desencriptarla.

Una vez hecho esto, el receptor utiliza la llave privada del emisor para desencriptar los datos y así poder conocerlos.

1.3. Firma Digital

Consisten básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la **identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la confidencialidad**. Los algoritmos de Clave Publica son los más utilizados en Firma Digital.

Una firma digital se utiliza para garantizar al receptor que los datos firmados vienen de la persona que los envió y que no ha sido alterado. Una firma digital esta compuesta por un par de llaves. Una llave utilizada para firmar conocida como llave privada de firma y otra para verificar conocida como llave publica de firma.

El proceso de Firma Digital conlleva los siguientes pasos:

→El emisor comienza el proceso aplicando una función o código de resumen (hash fuction) al texto o datos originales. Esta función de resumen es una Huella Digital de identificación única de los datos. En las siguientes ilustraciones se muestra el proceso de firma digital.

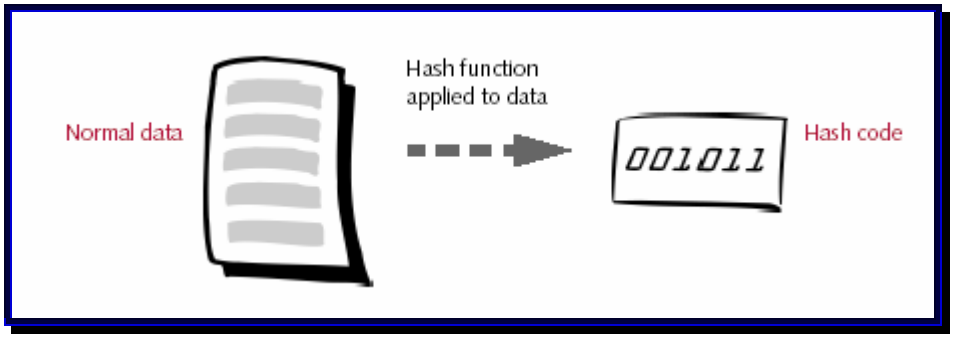


Ilustración I-7: Proceso de firma Digital Paso 1.

→ El emisor firma el código de resumen utilizando su llave privada de firma.

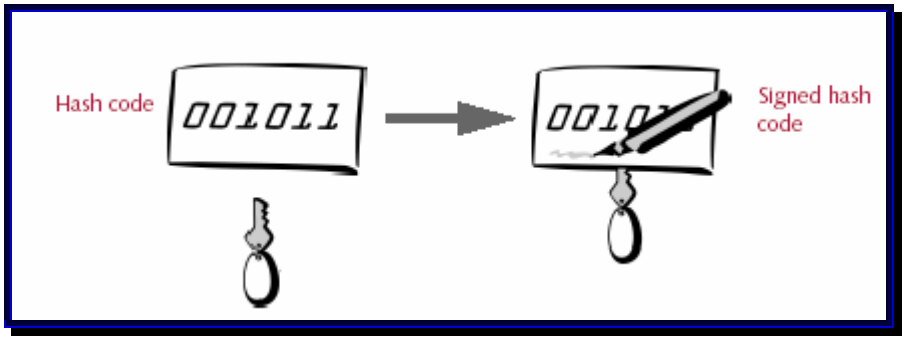


Ilustración I-8: Proceso de firma Digital Paso 2.

Cuando el emisor utiliza su llave privada para "Firmar " el código de resumen se considera una firma única, ya que solo él pudo haberlo hecho. Una vez que el emisor firma el código resumen lo envía junto al texto original al receptor, el cual realiza el proceso inverso conocido como verificación.

→ Una vez que el receptor recibe el texto original y el código resumen firmado, puede verificar que el emisor fue el que firmo el código resumen, recuperando (desencriptando) el código resumen utilizando la llave publica del emisor.

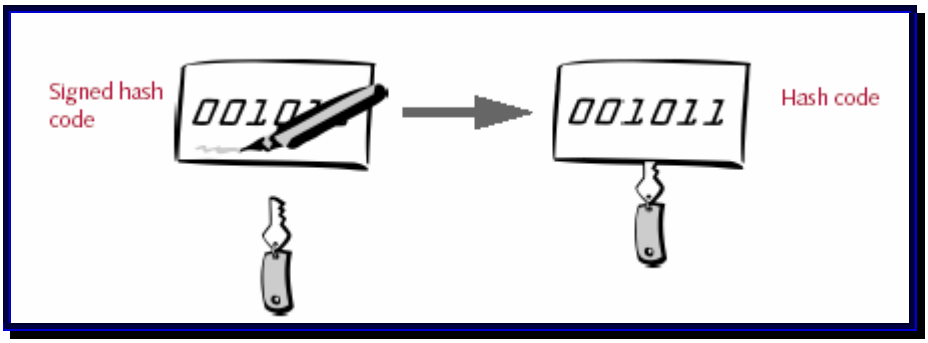


Ilustración I-9: Proceso de firma Digital Paso 3.

→ Una vez que obtiene el código resumen, el receptor aplica un nuevo código de resumen al texto o datos originales que tiene y lo compara con el obtenido del emisor. Si coinciden el texto puede considerarse como no alterado.

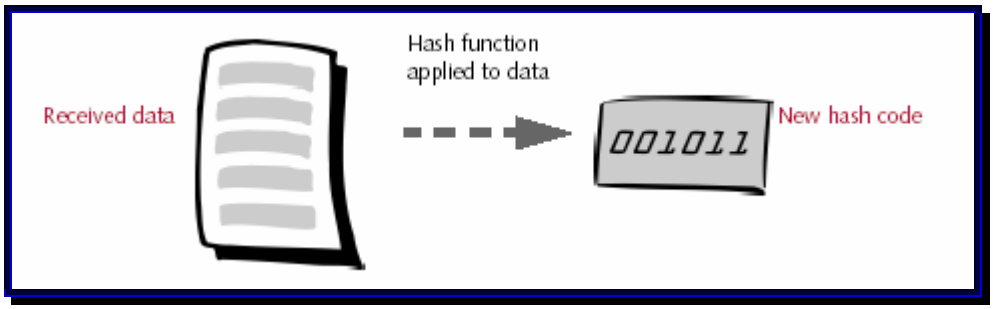


Ilustración I-10: Proceso de firma Digital Paso 4.

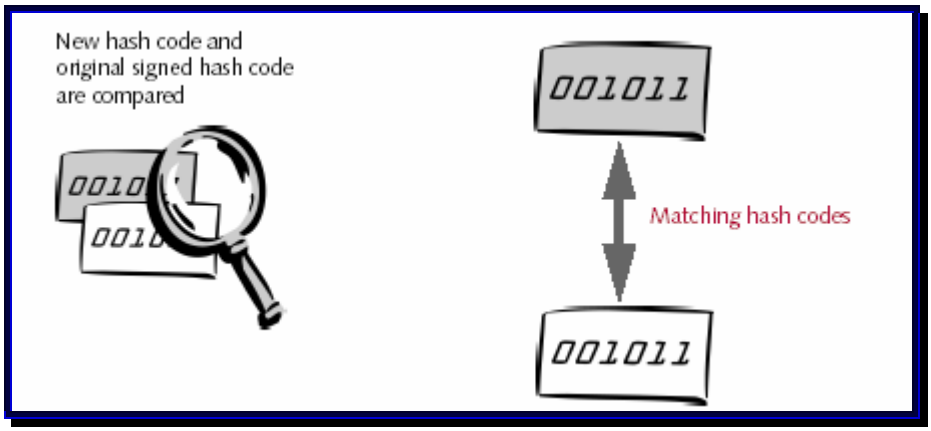


Ilustración I-11: Proceso de firma Digital Paso 5.

1.4. Llaves o Claves

Una llave o clave como también se le conoce, es un valor numérico de gran longitud que trabaja junto a un algoritmo criptográfico para producir texto cifrado. Una llave se mide en bits y mientras más grande sea, mayor será el nivel de cifrado para el texto.

2. Infraestructura de Clave Pública PKI

Como se describió anteriormente, la utilización de certificados digitales como método de autenticación de las VPN, requiere de la existencia de una infraestructura sobre el cual los certificados basen su funcionamiento. Esta infraestructura se le conoce con el nombre de Infraestructura de Clave Publica o PKI, y se basa en la utilización de tecnología de clave pública.

2.1. Definición

Existen varias definiciones de una PKI, pero la mas acertada, es la que nos brinda [RUSSEL-CRAWFORD00] quien la define como: "Un sistema de generación, administración, distribución y revocación de certificados de clave pública". El grupo de trabajo PKIX la define en su guía «Internet X.509 Public Key Infrastructure PKIX Roadmap», como "El conjunto de hardware, software, gente y procedimientos necesarios

para crear, manejar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública".

Una PKI brinda el marco para una amplia variedad de componentes, aplicaciones, políticas y prácticas que permiten combinar y obtener las cuatro principales funciones de seguridad para transacciones comerciales:

- Confidencialidad.
- Integridad.
- Autenticación.
- No repudiación.

2.2. *Funcionamiento básico de una PKI*

Una PKI emite un certificado digital acompañado de su correspondiente clave pública a usuarios y equipos a través de una Autoridad Certificadora AC, este certificado funciona como método de identificación. La llave privada correspondiente a la pública en el certificado es almacenada de manera local con altas medidas de seguridad. La AC se encarga también de colocar los certificados emitidos en un repositorio de certificado para que puedan ser verificados por aquellos que lo soliciten.

2.3. Componentes de una PKI

- Autoridad Certificadora AC. Representa la base de confianza de una PKI, ya que maneja los certificados de clave pública durante todo el ciclo de vida. La AC permitirá:

- Expedir certificados que garanticen la identidad de un usuario o sistema.
- Tener un calendario de fechas de expiración para los certificados.
- Garantizar que los certificados sean revocados cuando sea necesario, a través de Listas de Revocación de Certificados (CRL – Certificate Revocation List).

- Autoridades de Registro AR. En toda PKI deben establecerse los mecanismos para que los usuarios soliciten su propio certificado, de tal forma que se asegure la

identidad de dicho usuario, este proceso se conoce como registro de usuarios y es llevado a cabo por Autoridades de Registro.

Existen 2 tipos principales de registros:

- Registro Clásico: En el cual un usuario acude en persona a una oficina de registro, y tras verificar su identidad, se le proporciona de forma segura su clave privada y su certificado.

- Registro Remoto: En el cual un usuario solicita su clave privada y Certificado a través de Internet. Para esto se utilizara un software que será encargado de generar el par de claves, este a su vez envía la clave publica a la AR, para que sea firmada por la AC.

La validez de la Firma Digital estará condicionada por la calidad del proceso de registro, siendo obligatorio para asegurar la validez legal de la firma, algún tipo de registro "Cara a Cara", ya que es el único que asegura la identidad del solicitante. Por otra parte, la validez de la firma digital también estará condicionada a la firma manuscrita de un "contrato" por el que el solicitante acepta su certificado y las condiciones de uso del mismo.

La Autoridad de Registro estará conformada de una serie de elementos tecnológicos (hardware y software específicos) y medios humanos (los Operadores de Registro). Es el punto de comunicación entre los usuarios de la PKI y la Autoridad certificadora.

3. Políticas de Seguridad.

Las políticas de Seguridad definen el máximo nivel de seguridad de la información de una empresa, así como también los procesos y principios para el uso de la criptografía. Normalmente incluye normas sobre como manejar las llaves y la información valiosa para la organización, definiendo el nivel de control requerido para contrarrestar los riesgos. Dentro de las políticas de seguridad, se incluye un Reglamento de Certificados (CPS – Certificate Practice Statement) el cual se trata de un documento detallado que

contiene los procedimientos operativos de cómo debe ser reforzada y soportada la política de seguridad.

Normalmente un CPS incluye definiciones sobre cómo son construidos y operados los certificados, cómo son expedidos, aceptados y revocados, y cómo las llaves pueden ser generadas, registradas y certificadas, además de dónde serán almacenadas y cómo estarán disponibles para los usuarios.

4. Distribución de la Información en una PKI.

Dado que uno de los principales objetivos de una PKI es ofrecer información a los usuarios sobre los Certificados de los usuarios y sus correspondientes claves públicas, es un factor de vital importancia examinar la forma en que esta información se distribuye.

Los certificados ofrecen una buena forma de garantizar la correspondencia entre una clave pública y un usuario. Pero para que sean útiles, los usuarios deben poder acceder a ellos con comodidad y rapidez. Es importante además que puedan acceder a otra información relacionada con los certificados como es su estado de revocación, las políticas de certificación y certificados cruzados.

Las características más importantes de esta distribución son:

- Escalabilidad
- Eficiencia
- Disponibilidad
- Integridad

4.1. Métodos utilizados para la distribución de la información

✧Entrega Privada

Mediante el cual cada propietario de certificado es el encargado de distribuir su certificado a todos aquellos que lo necesiten. Una posible forma de realizar esta entrega sería mediante disquete. El propietario copia su certificado en un disquete y se lo entrega al

usuario que pueda necesitarlo, o también podría mandarlo como documento adjunto en un correo electrónico. Esto podría funcionar en una comunidad pequeña de usuarios en la que la todos los usuarios se conocen y pueden tener contacto directo, pero seria muy difícil en una comunidad mundial, por la dificultad de comunicación ente los usuarios.

✧Repositorio de Datos

Este representa el método mas utilizado, para publicar la información de una PKI. Un repositorio es una base de datos con una localización determinada y que puede ser accedida fácilmente. La información que se necesita distribuir se introduce en un repositorio y desde este puede ser accedida por los usuarios cuando la necesiten. Las tecnologías mas utilizadas para la creación de certificados son:

- LDAP (Protocolo de acceso ligero a directorios)
- Directorios X.500
- Servidores Web
- Servidores FTP
- Bases de Datos Corporativas.

Hay que tener en cuenta que en el repositorio no se almacena información que deba ser secreta, sino que el tipo de información que se almacena es toda pública, y no supone un problema que entidades ajenas a la PKI puedan acceder a ella. Sí que se debe proteger al sistema de accesos no autorizados para realizar modificaciones en la información contenida en el repositorio.

La localización del repositorio debe ser comunicada al usuario para que éste pueda acceder al mismo. Esta localización se expresará típicamente en forma de una dirección IP o de un nombre DNS. Esta dirección se debe comunicar al dar de alta un usuario en la PKI, y la forma de hacerlo dependerá de la forma en que se realice este proceso.

4.2. Métodos de acceso a repositorios.

El acceso externo a estos repositorios puede darse de diferentes maneras y va en dependencia de los niveles de seguridad que la implementación de la PKI requiera.

- *Acceso Directo*

En este modelo el acceso de una entidad externa a un repositorio se realiza directamente al mismo. Será adecuado cuando exista confianza entre ambas PKI o el repositorio esté protegido mediante algún mecanismo de autentificación.

- *Guardia*

Este método es similar al de acceso directo, con la diferencia de que se añade un mecanismo intermedio. Este mecanismo recoge las peticiones externas, realiza sobre ellas el control de acceso, obtiene la información pedida y la devuelve a la entidad externa.

- *Repositorio Compartido*

La existencia de un repositorio compartido posibilitaría que todas las PKI que necesiten interactuar publicasen su información en un único repositorio externo a todas ellas.

- *Repositorio Interdominio*

La replicación interdominio consiste en que cada PKI mantenga en su repositorio la información de los repositorios de las otras PKI. Cada PKI debe informar a las demás de los cambios en su repositorio y enviarles la nueva información.

- *Repositorio borde*

Esta técnica consiste en que cada PKI mantiene un repositorio externo a la red interna de la empresa. A este repositorio se le llama repositorio borde. De esta forma cada PKI mantiene dos repositorios, uno externo y uno interno. Las consultas de componentes de

la PKI se realizan al repositorio interno y las de elementos ajenos a las PKI al repositorio borde.

4.3 Aplicaciones Habilitadas para PKI

Son todas aquellas aplicaciones en las cuales es factible utilizar Certificados Digitales para la seguridad de las mismas. Entre estas aplicaciones tenemos: Comunicaciones entre Servidores y Navegadores Web, Intercambio Electrónico de Datos, VPN, Correo electrónico seguro.

4.4. Modelo de Confianza de una PKI

El gran número de usuarios que puede tener una PKI hacen que sea necesaria la existencia de varias AC en la misma, ya que el trabajo a realizar puede ser excesivo para una única AC. Estas AC deberán estar distribuidas de tal forma que permita determinar a las entidades finales en cuales de los certificados que les llegan pueden confiar. A la forma de realizar esta distribución se le llama modelo de confianza. Diremos que una entidad confía en un certificado cuando considera que el enlace especificado en el mismo entre una entidad y una clave pública es correcto.

Asimismo, una entidad confía en una AC cuando confía en todos los certificados emitidos por la misma. La emisión de certificados por parte de una AC que enlacen a otra AC con una clave pública permite que entidades que sólo confiaban en la primera AC pasen a confiar en la segunda.

- ✧ Herencia Estricta

En la herencia estricta, los componentes de la PKI se distribuyen en forma de árbol. En la raíz tendremos una AC a la que llamaremos AC raíz. En las hojas están las entidades finales. Entre ambos extremos tendremos una serie de niveles de nodos, que serán las AC intermedias.

En este esquema todos los componentes confían en la AC raíz. Después cada AC emite certificados para los componentes situados en nodos hijos de la misma. Así,

partiendo de un certificado emitido por la AC raíz se puede obtener un camino que lleve hasta un certificado emitido para una entidad final.

Para que se pueda comprobar la validez de un certificado, es necesario que cada componente de la estructura posea una copia de la clave pública de la AC. Esta clave debe ser distribuida por algún método seguro, de forma que no pueda ser modificada. Habitualmente este proceso necesitará el apoyo de algún mecanismo que funcione al margen de la red, como por ejemplo el correo convencional o el teléfono.

✧ Arquitectura Distribuida

En este modelo no se confía en una única AC raíz, sino que distintas entidades finales pueden tener su confianza depositada en distintas AC. Así se obtienen una serie de subestructuras independientes, que típicamente tendrán estructura de herencia estricta con una AC que funcionará como raíz en esa subestructura.

En el caso de que las subestructuras estén compuestas por una única AC y entidades finales, la configuración se llamará completamente igualada. En esta estructura todas las AC son independientes unas de otras. Si en cada subestructura hay más de una AC (hay AC subordinadas a otras) tendremos una configuración completamente arbolada.

✧ Certificación Cruzada

La certificación cruzada es un mecanismo utilizado para establecer una relación de confianza entre dos AC. Mediante la misma se puede conseguir que entidades que confían en certificados emitidos por una AC pasen a confiar también en los certificados emitidos por la otra AC. Diremos que una AC A certifica cruzadamente a otra AC B cuando firma un certificado que enlace a B con la clave pública de B. En la certificación cruzada se usan certificados.

En estos certificados tanto el sujeto como el emisor serán AC. Además, el uso de las extensiones de los certificados puede permitir incluir restricciones a esta relación, obteniendo así una relación de confianza con respecto únicamente a algunos de los

certificados emitidos por la otra entidad. La certificación cruzada puede ser unilateral o bilateral.

La certificación unilateral ocurre en un único sentido, es decir, una AC A certifica cruzadamente a una AC B, mientras que B no certifica cruzadamente a A. Este método se utiliza para establecer la herencia entre AC en las estructuras de árbol. En éstas la AC padre certifica cruzadamente a todas las AC que son hijas suyas La certificación bilateral se realiza en ambos sentidos. En este caso la AC A certifica cruzadamente a la AC B y al mismo tiempo B certifica cruzadamente a A. Este método se utiliza principalmente en la arquitectura distribuida para establecer la confianza entre dos subestructuras.

- ✧ Configuración en Red

En esta configuración se puede establecer certificación cruzada de cada AC raíz con todas las demás. En el caso de que se realice la certificación cruzada de todas con todas hablaremos de configuración en red completa. Si no hay certificación cruzada entre todas las AC raíz tendremos configuración en red parcial. Este tipo de configuraciones exigen un gran número de certificaciones cruzadas. En configuración en red completa se necesitan del orden de n2 certificaciones cruzadas, siendo n el número de AC raíz.

- ✧ Configuración Centralizada

En esta configuración tendremos una AC central con la que cada una de las AC raíz establecerá certificación cruzada. A la AC central se le suele llamar eje, y su función principal es la de interconectar las distintas infraestructuras. La ventaja de esta configuración frente a la anterior es que necesita menos certificaciones cruzadas.

- ✧ Modelo Web

Este modelo se diferencia de los anteriores en que la confianza no se deposita en una única AC, sino que se deposita en varias. En este caso también hay varias subestructuras, pero, a diferencia de la arquitectura distribuida, la entidad final deposita su confianza en todas las AC raíz. Podemos considerar este modelo como una extensión del de herencia estricta, en el que cada entidad final puede formar parte de varias estructuras.

✧ Modelo Centrado en el Usuario

En este modelo el encargado de decidir en que certificados se confía y en cuales no es directamente el usuario. Habitualmente cada usuario tendrá una serie de claves pertenecientes a conocidos en las que confiará. Cuando una entidad recibe un certificado, mira si algún certificado de la cadena de certificación asociada pertenece a algún usuario en el que confía directamente. Si no hay ninguno lo lógico es que rechace el certificado. Si hay alguno puede aceptarlo o rechazarlo, ya que puede considerar que el certificado en el que sí confía está demasiado lejos en la cadena de certificación. En todo caso, la decisión final es siempre del usuario. Este modelo puede funcionar bien en comunidades pequeñas de usuarios con altos conocimientos técnicos, pero no es adecuado para comunidades normales de usuarios.

4.5. Certificados Digitales

Un certificado digital es un archivo de aproximadamente 1k de tamaño, que contiene, los datos del propietario, su clave pública y la firma digital de una autoridad competente. Cuando una persona solicita un certificado digital, se generan su par de claves, la pública y la privada. La clave pública viene en el certificado digital explícitamente. La clave privada queda en custodia del propietario del certificado. El tercer elemento importante que tiene el certificado digital es la firma digital de una autoridad certificadora, quien es el que otorga el aval de que los datos corresponden al propietario.

Un Certificado Digital contiene:

- Los datos Identificativos del solicitante.
- La fecha de expedición y la de revocación.
- La clave pública del solicitante.
- Un numero secuencial Identificativo.
- La firma digital de la autoridad certificadora.

4.5.1. Formato de certificados digitales

En la actualidad tenemos un formato (estándar) que se ha extendido casi para todas las aplicaciones, este es el llamado X.509. Un certificado X.509 consiste en la clave pública del usuario y la firma de un tercero para la identificación en el bloque de información de ese usuario. Este tercero (Autoridad Certificadora AC) puede ser una agencia gubernamental, una institución financiera o incluso un servidor confiable dentro de la oficina.

El usuario le da a la AC su clave pública y esta responde con un certificado. La norma X.509 también incluye otros elementos como un identificador que indica el algoritmo empleado para firmar el documento, y la fecha de expiración del certificado. La mejor propiedad del formato X.509 es que contiene el mínimo necesario de información para poder realizar muchas transacciones, principalmente comerciales y financieras. Sin embargo para otras aplicaciones puede ser un poco robusto.

4.5.2. Validación de un Certificado

Este es el proceso mediante el cual se asegura que la información que contiene el certificado es aún valida. En este proceso tanto el usuario puede consultar a la AC la validez del certificado cada vez que lo necesite, así como también la AC puede incluir información de validez en el mismo certificado.

4.5.3. Revocación de un Certificado

Este es el proceso mediante el cual se informa a los usuarios de que la información de un certificado ya no es valida (ya sea por robo, alteración o cambios en los datos del usuario). El método más común para la revocación de un certificado consiste en publicar dicho certificado en una Lista de Revocación de Certificados conocida como CRL (Certificate Revocation List), que maneja cada AC para los certificados que emite y firma.

4.5.4. Manejo de Llaves

Los pasos que conllevan el manejo de las Llaves son:

→ Generación de la Llave: Los pasos que se siguen para la generación de las llaves son:

- Se da la identificación del usuario.
- La AC envía información secreta al usuario.
- La generación del par de llaves se lleva a cabo, ya sea por el usuario o por la AC.
- Se establece una conexión entre el usuario y la AC de tal manera que la clave privada se envía al usuario, mientras que la publica a la AC.

→ Almacenamiento de Llaves Privadas: Se recomienda que las llaves privadas sean almacenadas en dispositivos de almacenamiento seguros. La llave privada de la AC debe ser protegida rigurosamente y almacenada en dispositivos a prueba de fuego, agua ya que si esta se ve comprometida se pierde la infraestructura completa.

→ Revocación de Llaves Públicas: Este proceso debe ser bastante fácil, pero a su vez seguro.

→ Publicación de Certificados y Listas de Revocación: Debido a que la AC firma tanto los Certificados como las CRL, estos son resistentes a alteraciones, y pueden darse a conocer a través de: Publicación en un directorio LDAP/X.509, transferencia directa a quien lo solicite, publicarlo en un sitio Web.

→ Actualización de Llaves: Debido a que los certificados tienen un tiempo de vida limitado se requiere un proceso para actualizar el par de llaves de los usuarios así como un nuevo certificado.

→ Backup / Recuperación: Esta función permite recuperar la llave privada de un usuario, cuando este la pierde. La recuperación de ésta es realizada por una AC, la cual mantiene una base de datos de las llaves Privadas de todos los usuarios.

II. ANALISIS COSTO BENEFICIO

II. ANALISIS COSTO BENEFICIO

A. Factibilidad Técnica

1. Situación Actual

Actualmente tanto la SEJUVE como el SNIP poseen una infraestructura de red interna que permite la intercomunicación de todos sus usuarios. La SEJUVE cuenta con dos servidores IBM con procesador XEON. Un servidor principal que funciona como controlador de dominio, servidor de correo, servidor Web y utiliza Windows 2000 Server como Sistema Operativo y un servidor secundario que funciona como enrutador y Firewall y utiliza el SO (Sistema Operativo) LINUX. La SEJUVE cuenta además con una conexión a Internet por cable-MODEM con una velocidad de 256 K.

El SNIP cuenta con un rack de servidores DELL con procesadores XEON utilizados de forma similar para correo, controlador de dominio, servidor de aplicaciones y servidor WEB haciendo uso del SO Windows 2000 Server. También utilizan un equipo de características similares como enrutador y Firewall utilizando LINUX como SO. El SNIP cuenta con una conexión por radio-MODEM (inalámbrica) de 2 mbps.

2. Necesidades de Interconexión

La Secretaría de la Juventud requiere de un mecanismo de comunicación que permita a los usuarios del SNIP acceder a la red de área local de la SEJUVE desde sus instalaciones físicas emulando **un enlace punto a punto** de tal manera que se facilite la transferencia de información concerniente al seguimiento de programas y proyectos que la SEJUVE administra y que el SNIP supervisa, y que a la vez sea un mecanismo económico, seguro y flexible.

A través de los últimos años y con el desarrollo de las comunicaciones se han visto varias alternativas que podrían satisfacer las necesidades que se plantean. El inconveniente con estas alternativas son los elevados costos, esto impide que algunas organizaciones puedan implementarla. Ejemplos de este tipo son las líneas dedicadas y acceso remoto por teléfono.

Recientemente han surgidos nuevas tecnologías de comunicación que podrían ser soluciones viables para cubrir las necesidades que presentan las instituciones mencionadas. Entre estas tecnologías tenemos: **Inalámbrica o por radio-MODEM y VPN**. Sin embargo la tecnología VPN promete ser una solución segura y de menor costo que la inalámbrica, que podría implementarse en empresas u organizaciones que deseen interconectar sus redes locales con el propósito de agilizar la transferencia de información.

3. Análisis comparativo entre la tecnología inalámbrica y VPN.

Uno de los objetivos del presente estudio monográfico es demostrar que la implementación de una VPN provoca ahorros en compra y mantenimiento de equipos y ahorros en costos de comunicación en comparación con la tecnología inalámbrica punto a punto que ofrecen actualmente la mayoría de los proveedores de Internet en Nicaragua tales como IBW, IFX , IDEAY, NEWCOMS AMERICA.

La demostración se realizará a través de un estudio que incluye Factibilidad Técnica, Factibilidad Operacional, Factibilidad Económica y un análisis costo beneficio para reflejar los beneficios que la implementación de una VPN trae a las organizaciones.

Debido a que la descripción de los detalles de la infraestructura de red interna de cada una de las instituciones esta fuera del alcance de este estudio no será incluido en el análisis comparativo, el cual se centrará únicamente en la comparación de las dos alternativas propuestas para lograr el enlace punto a punto.

3.1. Requerimientos de Implementación

- Enlace Punto a Punto Inalámbrico:

a) Grafico Ilustrativo de la Solución.

En la ilustración II-1 se puede apreciar que la SEJUVE utilizaría una conexión por cable MODEM para acceder a Internet y una conexión Inalámbrica para el enlace P.P las cuales estarían conectadas al enrutador principal, y es por medio de este que se permite

el acceso a la red interna. De forma similar el SNIP utiliza dos conexiones inalámbricas, una para el enlace a Internet y la otra para el enlace P.P

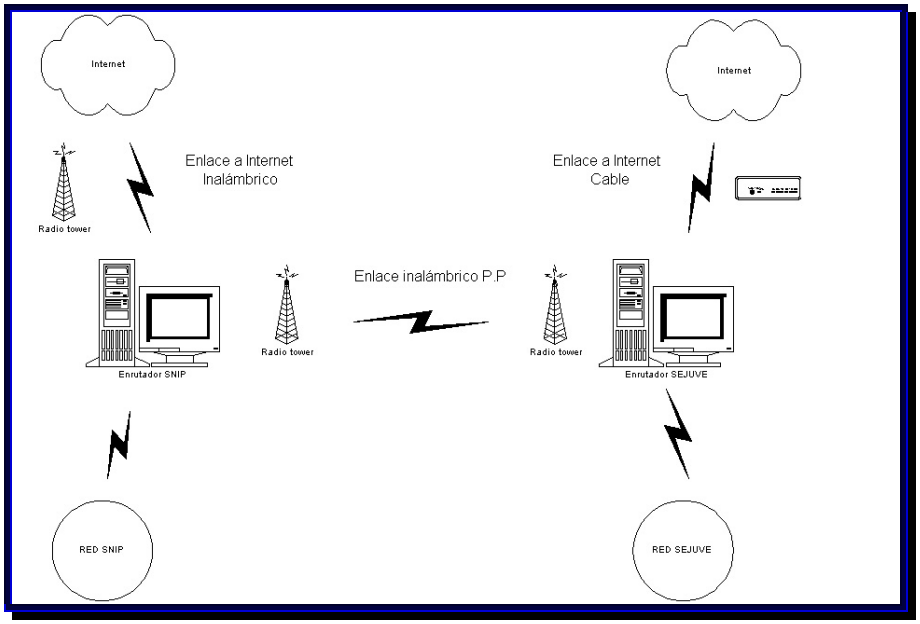


Ilustración II-1: Gráfico ilustrativo de la solución inalámbrico

Como se logra apreciar en el gráfico con esta solución se requiere que ambas instituciones tengan enlaces separados para Internet y el enlace dedicado P.P.

b) Equipos de Comunicación para la SEJUVE

Los equipos que se describen en la Tabla II-1 y II- 2 manejan tanto el enlace de Internet como el enlace P.P utilizando tecnología Inalámbrica.

Tabla II-1: Equipos de Comunicación para SEJUVE. Enlace Inalámbrico

Equipo	Cantidad	Observaciones
Antena Semi-Parabólica	1	Se utilizan para el enlace P.P
Torre	1	
Radio MODEM	1	
Cable MODEM	1	Enlace a Internet
Enlace Internet	1	256 Kbps
Enlace P.P.	1	512 Kbps

c) Equipos de Comunicación para el SNIP

Tabla II-2: Equipos de Comunicación para el SNIP. Enlace inalámbrico.

Equipo	Cantidad	Observaciones
Antena Semiparabólica	2	Se utilizan para el enlace P.P. Enlace a Internet
Torre	1	
Radio MODEM	2	
Enlace P.P.	1	512 Kbps
Enlace Internet	1	256 Kbps

- Enlace VPN:

a) Grafico Ilustrativo de la Solución.

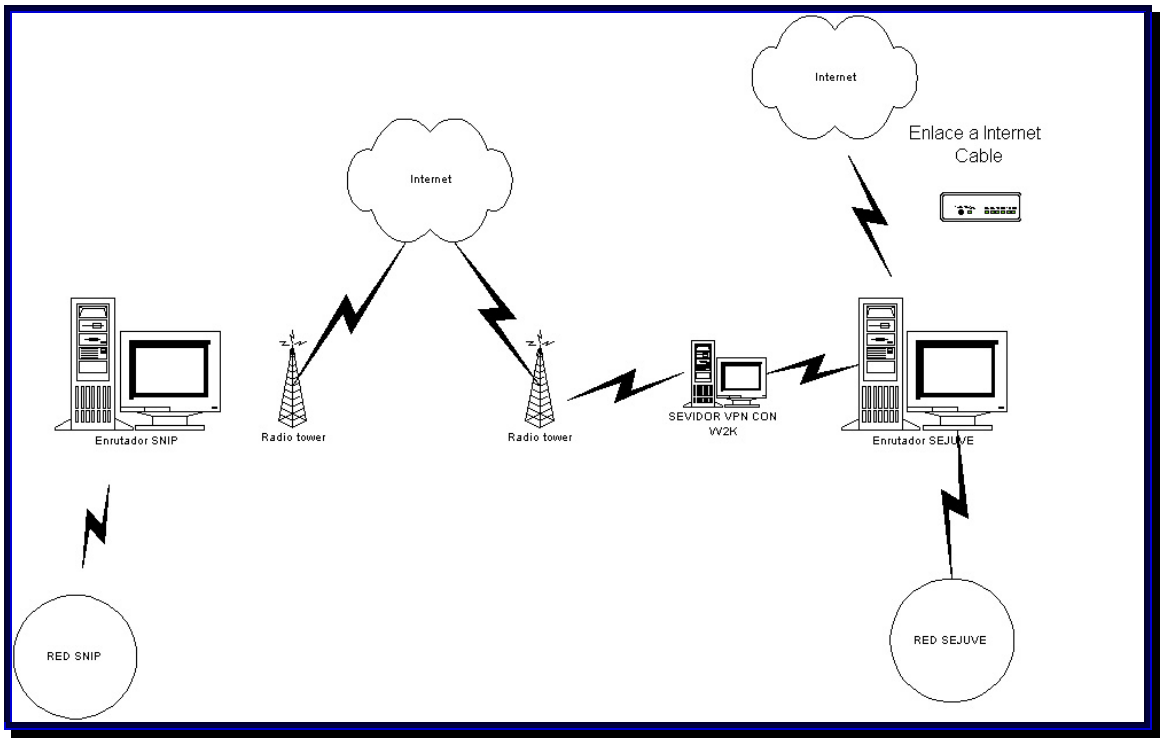


Ilustración II-2: Gráfico ilustrativo de la solución VPN.

Como se logra apreciar en el gráfico con esta solución, el SNIP utiliza la misma conexión de Internet (inalámbrica) para realizar el enlace punto a punto con la SEJUVE y tener acceso a Internet. Por el otro lado la SEJUVE utiliza un conexión por cable MODEM para acceder a Internet y una conexión inalámbrica para el enlace P.P.

b) Equipos de Comunicación para la SEJUVE

Los equipos que se describen en la Tabla II- 3 y II-4 manejan tanto el enlace de Internet como el enlace P.P utilizando VPN.

Tabla II-3: Equipos de Comunicación para la SEJUVE. Enlace VPN.

Equipo	Cantidad	Observaciones
Cable MODEM	1	Enlace a Internet
Enlace Internet	1	256 K
Antena Semi-Parabólica	1	Enlace P.P.
Torre	1	
Radio MODEM	1	
Enlace P.P.	1	512 Kbps

c) Equipos de Comunicación para el SNIP

Tabla II-4: Equipos de Comunicación para el SNIP. Enlace VPN.

Equipo	Cantidad	Observaciones
Antena Semi-Parabólica	1	Se utilizan para el enlace P.P. Enlace a Internet
Torre	1	
Radio MODEM	1	
Enlace Internet	1	256 Kbps 512 Kbps Nacional

d) Hardware

La tabla II-5 describe el equipo necesario para la implementación de la VPN.

Tabla II-5: Hardware en enlace VPN.

Categoría	Elemento	Componentes	Requerimientos
Hardware	**Servidor VPN**	Procesador	Amd, Celeron o Intel de 1 Ghz como mínimo.
		Memoria Ram	256 Mb Tipo DDR
		Puertos	Serial, Para, Usb
		Ranuras	3 PCI como mínimo
		Disco Duro	30 GB SCSI
		Unidad de Cd	52 x
		Auto restauración	Soportada
		Tarjetas de Red	10/100
	UPS/Estabilizador	Capacidad	750 VA
		Voltaje Nominal	120 V I/O
		Tomas para Estabilizador	2
		Tomas para Batería	2
		Tipos de Protección	Internet, Fax , MODEM

3.2. Opción Recomendada

Según los requerimientos técnicos descritos anteriormente es fácil darse cuenta que técnicamente es más factible implementar la tecnología VPN, ya que requiere de menos equipos y enlaces, lo que provoca una considerable disminución en los costos.

B. Factibilidad Operativa

La implementación de una Red Privada Virtual entre la SEJUVE y el SNIP, tendrá un gran impacto para los usuarios de las dos instituciones, ya que se les facilitará el proceso de transmisión de información y de igual manera se podrá agilizar las siguientes tareas:

- Seguimiento en el desarrollo de los Programas y Proyectos concernientes a Juventud por parte del SNIP.

- Actualización de manera inmediata de la base de datos del banco de proyectos, cuando esta presente fallas.

Esto trae como consecuencia que las decisiones que se tomen se realicen con mayor rapidez elevando de esa manera el rendimiento y la productividad de ambas instituciones.

1. Alcance y Oportunidad

La implementación de toda tecnología informática en una organización provoca cambios en la forma habitual de realizar las tareas, por lo cual es muy importante considerar factores como la resistencia al cambio y el tiempo de asimilación de la nueva tecnología, parámetros que nos indican si la tecnología a implementar es operativamente factible.

El hecho de que ambas instituciones permitan a sus usuarios utilizar sus respectivas Lan para acceso a Internet de manera permanente, provoca que tanto los usuarios de la SEJUVE como los del SNIP sean personas con cierta experiencia en el manejo de sistemas que incluyan la utilización de la Internet como medio de comunicación, por lo que se deduce que presentaran poco resistencia al cambio.

De igual forma se espera que la curva de aprendizaje de la tecnología por parte de los usuarios de ambas instituciones sea corto debido en primer lugar a la experiencia comprobada de los usuarios y en segundo lugar a la capacitación que se les dará.

El alcance de la VPN que se pretende en este estudio está orientado para todos los usuarios que estén relacionados con el manejo de programas y proyectos que la SEJUVE ejecuta y la contraparte del SNIP encargados de la supervisión de los mismos.

2. Dotación

La implementación de una VPN requiere de cierto personal que se encargue de la administración y mantenimiento de la misma. Esta tarea puede ser realizada por el personal encargado de la administración de la red del Departamento de Informática cuando la organización no sea tan grande, pero en aquellos casos en que la organización sea considerada como grande, se deberá contratar a un administrador de red exclusivo para el manejo y mantenimiento de la VPN.

En la SEJUVE esta tarea puede ser realizada perfectamente por el departamento de Informática, pero para efectos demostrativos se detallará el cargo y funciones que debe realizar la persona que se contrate para la administración de la VPN cuando se requiera. Es importante aclarar que debido a esto último no se tomará en cuenta la dotación de personal en la cuantificación económica.

Tabla II-6: Cargos y Funciones Administrativas de la VPN.

Cargo	Perfil	Funciones
Administrador de la VPN	Administrador de Redes	Velar por el buen funcionamiento de la VPN.
		Velar por que los usuarios hagan uso de la VPN exclusivamente para asuntos laborales.
		Dar Asistencia a los Usuarios en el uso de la VPN.

El administrador de la VPN dependerá por completo del Administrador de la Red General y deberá coordinarse con este para cualquier cambio o mantenimiento que se pretenda realizar.

C. Factibilidad Económica

Este apartado está enfocado en demostrar que la VPN no sólo es factible técnicamente, sino también económicamente, al incurrir en menos costos por adquisición, mantenimiento de equipos y enlaces de comunicación.

1. Cuantificación de la Inversión

En esta cuantificación se tomaran en cuenta exclusivamente todos los elementos que se necesitan para lograr que ambas instituciones cuenten con acceso a Internet y la vez un enlace P.P. que permita la transmisión de información de manera fácil y rápida.

Las cantidades que se incluyen en las tablas están representadas en moneda americana, (US $ dólares americanos), debido a la devaluación de la moneda Nacional con respecto a ésta.

1.1. Enlace P.P. utilizando tecnología inalámbrica dedicada.

- Costos por Instalación de equipos:

Tabla II-7: Costos de Instalación de equipos.

Concepto	Lugar	Costo Total $
Cable MODEM	**SEJUVE**	0.00
Enlace Inalámbrico	**SEJUVE**	500.00
Enlace Inalámbrico	**SNIP**	500.00
	Total	1000.00

- Costos de Enlaces Recurrentes por enlace privado:

Tabla II-8: Costos de Enlaces Recurrentes

Concepto	Lugar	Velocidad	Costo Total $
Enlace a Internet	**SEJUVE**	256 K	300.00
Enlace a Internet	**SNIP**	256 Kbps	800.00
Enlace P.P.	**SEJUVE**	512 Kbps	800.00
Enlace P.P.	**SNIP**	512 Kbps	800.00
		Total	2700.00

- Costos de Implementación del enlace privado:

Tabla II-9: Costos de Implementación del Enlace Privado.

Concepto	Cantidad	Lugar	Costo Unitario $	Costo Total $
Torre	1	**SEJUVE**	1250.00	1250.00
Radio MODEM/Antena	1		4000.00	4000.00
Cable MODEM	1		89.00	89.00
			Total	**$ 5339.00**

Concepto	Cantidad	Lugar	Costo Unitario $	Costo Total $
Torre	1	**SNIP**	1250.00	1250.00
Radio MODEM/Antena	2		4000.00	8000.00
			Total	**$ 9250**

- Costos de Mantenimiento de Equipos del enlace privado:

Tabla II-10: Costos de Mantenimiento de equipos del Enlace Privado.

Concepto	Modalidad	Lugar	Costo Total $
Mantenimiento de Equipos	Semestral	**SEJUVE**	250.00
		SNIP	250.00
		Total	$ 500.00

1.2. Enlace P.P. utilizando tecnología VPN.

- Costos por Instalación de equipos:

Tabla II-11: Costos por Instalación de equipos. Tecnología VPN.

Concepto	Lugar	Costo Total $
Cable MODEM	**SEJUVE**	0
Servidor VPN	**SEJUVE**	100.00
Enlace Inalámbrico	**SEJUVE**	500.00
Enlace Inalámbrico	**SNIP**	500.00
	Total	1100.00

- Costos de Enlaces Recurrentes:

Tabla II-12: Costos de Enlaces Recurrentes. Tecnología VPN.

Concepto	Lugar	Velocidad	Costo Total $
Enlace a Internet	**SEJUVE**	256 K	300.00
Enlace a Internet	**SNIP**	512 Kbps	800.00
Enlace P.P.	**SEJUVE**	512 Kbps	800.00
		Total	**1900.00**

- Costos de Implementación:

Tabla II-13: Costos de Implementación. Tecnología VPN.

Concepto	Cantidad	Lugar	Costo Unitario $	Costo Total $
		SEJUVE		
Cable MODEM	1		89.00	89.00
Servidor VPN	1		460.00	460.00
Licencia de Windows 2000 Server	1		90.00	90.00
Torre	1		1250.00	1250.00
Radio MODEM/Antena	1		4000.00	4000.00
			Total	**$ 5889.00**
Concepto	**Cantidad**	**Lugar**	**Costo Unitario $**	**Costo Total $**
		SNIP		
Torre	1		1250.00	1250.00
Radio MODEM/Antena	1		4000.00	4000.00
			Total	**$ 5250.00**

- Costos de Mantenimiento de Equipos:

Tabla II-14: Costos de Mantenimiento de equipos. Tecnología VPN.

Concepto	Modalidad	Lugar	Costo Total $
Mantenimiento de Equipos	Semestral	**SEJUVE**	0
		SNIP	250.00
		Total	**$ 250.00**

2. Análisis Comparativo de Costos

Tabla II-15: Análisis Comparativo de Costos.

Concepto	Enlace Inalámbrico P.P.	VPN
Costo de Instalación	1000.00	1100.00
Costos Concurrentes (Mensuales)	2700.00	1900.00
Implementación	14589.00	11139.00
Costo por Mantenimiento de Equipos (Semestral)	500.00	250.00
Costo Totales	**18789.00**	**14389.00**

Como se logra apreciar en las tablas anteriores la implementación de una VPN provoca un ahorro sustancial de costos de $5,160.00 dólares aproximado al 30%, en comparación con un enlace inalámbrico P.P., quedando demostrado de esta manera que la VPN es una solución económicamente más factible ya que provoca ahorros significativos.

3. Cronograma de Implementación de la VPN.

Tabla II-16: Cronograma de Implementación de la VPN.

Numero	Tarea	Lugar	Duración (Días)
1	Instalación de Elementos Físicos	SEJUVE-SNIP	3
2	Instalación de Enlaces	SEJUVE-SNIP	5
3	Configuración de Servidor VPN	SNIP	2
4	Configuración de Clientes VPN	SEJUVE	2
5	Pruebas de Conectividad	SEJUVE-SNIP	3
		Total	**15**

El total de días presentado en el cronograma de implementación esta basado en periodos laborables hábiles considerando como horario de trabajo de Lunes a Viernes de 08:00 AM a 5:00 PM.

D. Análisis Costo Beneficio

1. Costos

Implementar una VPN no significa que los costos de comunicación se reducen a 0, como se puede apreciar se necesitan $14389.00 dólares para poder desarrollarla. La implementación de una VPN más bien significa, utilizar una tecnología más barata y más simple que puede realizar el mismo trabajo y tener el mismo desempeño que se obtiene al utilizar una tecnología más cara y sofisticada.

2. Beneficios

Ahorro en costos: Una de las principales razones, por la cual las VPN están siendo altamente utilizadas es debido a que reducen los costos de comunicación en un gran porcentaje en comparación a las tecnologías anteriormente utilizadas como Frame Relay, o Líneas Dedicadas.

Esto significa que con una VPN una empresa puede utilizar una simple conexión a Internet, la cual es relativamente barata, y permitir a sus usuarios, proveedores, u otros usuarios acceder de manera rápida y eficiente a su red interna para agilizar la transferencia de información.

Seguridad: La tecnología VPN provee niveles de seguridad elevados mediante la utilización de técnicas avanzadas de encriptación, creación de túneles y autenticación.

Escalabilidad: La tecnología VPN es considerada escalable porque permite agregar n cantidad de usuarios y servicios sin la necesidad de cambios relevantes de infraestructura.

Compatibilidad con Tecnologías de Banda Ancha: Esto significa que una VPN no esta regida por la utilización de una tecnología de banda ancha (MODEM, DSL, RADIO-MODEM) en específico, sino más bien la que más se adecue a sus necesidades reales.

Incremento de la Productividad: La productividad es de suma importancia para cualquier empresa. Mediante la utilización de una VPN una empresa incrementa su productividad al permitir que la información viaje y sea compartida por los diferentes componentes de manera rápida y eficiente.

III. Análisis y Diseño de una VPN

III. ANALISIS Y DISEÑO DE UNA VPN

La implementación de cualquier tecnología informática requiere de un previo análisis y diseño que permita conocer a fondo la tecnología y realizar un esquema previo que permita lograr el objetivo final de la mejor manera posible.

El proceso para poder llevar a cabo la implementación de una VPN con certificados digitales consta de 6 fases o etapas las cuales se describen a continuación:

- Análisis de la VPN
- Diseño de la VPN
- Implementación de la VPN
- Análisis de una PKI
- Diseño de una PKI
- Implementación de una PKI

Debido a que para poder implementar la VPN con certificados se requieren que los equipos involucrados ya tengan instalados los correspondientes certificados, el orden en el proceso de implementación se modificara de la siguiente manera:

Análisis de la VPN
Diseño de la VPN
} FASE I

Análisis de una PKI
Diseño de una PKI
Implementación de una PKI
} FASE II

Implementación de la VPN con Certificados
} FASE III

A. Análisis

1. Infraestructura de Comunicación Básica para una VPN.

La utilización de una VPN para la transferencia de información con otras instituciones o empresas tiene como requisito indispensable la utilización de la Red Internet para lograr el enlace.

En Nicaragua existen dos alternativas para acceder a Internet a) Utilizando tecnología de acceso telefónico a redes (línea telefónica) b) Utilizando tecnología de acceso permanente (radio-MODEM, cable-MODEM).

Para hacer uso de la VPN a través de una **línea telefónica** se debe constar con los siguientes elementos:

a) Usuario o Cliente

- Computadora IBM compatible.
- Software o SO con capacidad para creación de túneles (Win 2000, Win XP).
- Un MODEM interno o externo de 56 Kbps.
- Línea Telefónica.
- Poseer una cuenta de acceso a Internet con un Proveedor de Servicios.

b) *Para el Servidor VPN*

- Equipo para el Servidor VPN.
- Dirección IP Pública Única.
- Acceso a Internet Permanente.
- Software o SO con capacidad para autenticación de usuarios, manejo de túneles y manejo de algoritmos de encriptación.
- Infraestructura Típica de una Lan.

De forma similar se requiere de los siguientes elementos cuando se desee utilizar VPN con **tecnología de acceso permanente.**

a) Usuario o Cliente en la red Interna

- Computadora IBM compatible.
- Servidor con software que permita conexión compartida a Internet, incluyendo los dispositivos necesarios para lograr este acceso (radio-MODEM, cable-MODEM).
- Infraestructura Típica de una Lan.

b) Usuario o Cliente conectado directamente a Internet

- Computadora IBM compatible.
- Software con capacidad para creación de túneles.
- Acceso dedicado a Internet incluyendo los dispositivos necesarios para lograr este acceso (Cable MODEM, Radio MODEM).

c) *Para el Servidor VPN*

- Equipo para el Servidor VPN.
- Dirección IP Pública Única. (Asignada por el proveedor de Servicios)
- Acceso a Internet Permanente.
- Software o SO con capacidad para autenticación de usuarios, manejo de túneles y manejo de algoritmos de encriptación.
- Infraestructura Típica de una Lan.

Los elementos necesarios en todas sus variantes representan las infraestructuras básicas de comunicación con la que se debe constar cuando se desea implementar una VPN.

La empresa u organización que desee implementar una VPN deberá considerar bien sus necesidades en contraste con las opciones disponibles para seleccionar la más adecuada.

2. VPN mediante Software y VPN mediante Hardware.

Una VPN puede ser implementada a través de Hardware y a través de Software. Muchos especialistas en la materia han discutido ampliamente para decidir cual es la mejor opción, pero han llegado a la siguiente conclusión como dice [1]Michael G. Barroga, "No existe una implementación de VPN que sea adecuada para todas las situaciones, cada una de ellas tiene sus propias ventajas y desventajas y depende mas bien del escenario en que se implemente ".

En las tablas III-1 y III-2 se presentan algunas ventajas y desventajas que se pueden apreciar al implementar una VPN tanto en Software como en Hardware.

Software VPN

Tabla III-1:Software VPN

Ventajas	Desventajas
Bajo Costo	Poco desempeño cuado se utiliza en un equipo que maneja varios procesos.
Escalable	Permite agregar cualquier servicio adicional cuando se requiera.
Flexible	No hay cambios en la infraestructura de Red
Se requiere de menos Capacitación	

Hardware VPN

Tabla III-2: Hardware VPN

Ventajas	Desventajas
Alto Desempeño	Infraestructura de Red mas compleja
	Se requiere de mayor capacitación
	Mayores Costos

[1] N*etwork Development Engineer Philippine Computer Storage Services, Inc*

Como se puede observar en las anteriores tablas, cuando se utiliza una VPN mediante Hardware requiere de equipos propietarios de ciertas compañías como Cisco Systems cuyo costo, configuración y manejo son elevados ya que se requiere que sean llevadas a cabo por especialistas de la misma compañía, además si se daña alguna pieza esta tiene que ser remplazada por una igual y no por la de otro fabricante. Su implementación se recomienda en grandes empresas donde el desempeño, juega un papel importante.

Por otro lado, la implementación de una VPN utilizando Software, representa una alternativa más económica y viable para empresas u organizaciones pequeñas donde no se requiere un alto desempeño pero sí la disminución en costos. Este tipo no requiere de actualización de equipos, ni se necesitan implementar equipos que puedan modificar la infraestructura de red con que se cuenta y que requieran de una capacitación especializada.

Esta comparación de ventajas y desventajas entre ambos tipos de implementación nos permite decidir que la implementación de la VPN en este estudio se llevará a cabo utilizando **Software** principalmente por las siguientes razones:

- La SEJUVE y el SNIP cuentan con SO clientes que tiene la capacidad para crear y manejar conexiones VPN, por lo que no se necesita software adicional.

- Ambas Instituciones cuentan con SO de servidor que tienen la capacidad para manejar clientes VPN, por lo que no se necesita software adicional.

- La configuración tanto del Servidor como de los Clientes VPN requiere de poca capacitación, ya que se el personal de informática de ambas instituciones poseen basta experiencia en el manejo de estos sistemas.

- La implementación de VPN mediante software es una solución más económica que la utilización de hardware propietario.

El software que se utilizará para la VPN, es el Sistema Operativo Windows 2000 Server (W2K), este no es el único software disponible para la implementación de una VPN en el mercado, pero si un software bastante completo que es compatible con la mayoría de los protocolo estándares para la creación de túneles, y algoritmos de

encriptación y que además permite utilizar certificados digitales como uno de sus métodos de autenticación para aplicaciones cliente/servidor como la VPN.

Otras alternativas para la creación de VPNs son Power VPN y Check Point VPN-1 pero presentan algunas desventajas en comparación con Windows 2000 entre las que se destacan: primero la incapacidad de la solución Power VPN para manejar certificados basados en el estándar X. 509v3, y segundo la incapacidad de ambas soluciones para manejar múltiples protocolos para túneles, el cual crea un inconveniente para aquellos clientes que sólo soportan un tipo especifico de protocolo para túneles y no tres como W2K (PPTP, L2TP y IPSEC). La tabla III-3 muestra una breve comparación de las soluciones alternativas para la implementación de una VPN.

Tabla III-3: Otras Alternativas en Software para VPN.

Características	Power VPN	Check Point VPN-1
Numero de Túneles Soportados	25, 50,100 según Lic.	Sin Limite
SO del Cliente	Windows 95 Windows NT, Windows 98, Windows 2000	Windows 95. 98. NT. 2000. ME
Protocolo de Manejo de Llaves	IKE	SKIP
Algoritmos de Autenticación	HMAC MD5, HMCAC SHA-1, Null	HMAC MD5, HMCAC SHA-1.
Algoritmos de Encriptación	DES, Triple DES, Null	DES. Triple DES. RC5. RC4. CAST
Soporte para Certificados	Solo para Certificados Entrust	Baltimore Technologies. Data Key. Entrust. IPlanet. RSA Security. VeriSign
Protocolos de Túneles	IPSEC	IPSEC

3. VPN en Windows 2000 Server

Como se mencionó anteriormente, una VPN es la extensión de una red privada utilizada para enlazar sitios geográficamente distintos a través de un enlace público o compartido como el Internet y emular un enlace punto a punto.

Windows 2000 Server es un Sistema Operativo que posee dentro de sus componentes un módulo denominado RRAS por sus siglas (Rounting Remote Access Service) mediante el cual tiene la capacidad para poder crear una VPN.

4. Tipos de VPN en Windows 2000 Server

Utilizando Windows 2000 Server una VPN puede ser implementada de dos diferentes maneras:

a) Conexión VPN de Acceso Remoto: La cual es llevada a cabo por un cliente de acceso remoto que se conecta a una red privada. El servidor VPN permite que el cliente de acceso remoto acceda, tanto a sus recursos como a los de la red privada a la que este conectado dicho servidor. La información que atraviesa la conexión VPN es originada por el cliente de Acceso Remoto, éste a su vez se autentica ante el servidor VPN, y de igual forma lo hace éste ante el cliente.

b) Conexión de Enrutador a Enrutador: En la cual la conexión VPN se realiza entre dos enrutadores (Servidores) que se encargan de conectar dos porciones de la red privada. El primer servidor VPN provee una conexión enrutada a la red en la cual está conectada el segundo servidor VPN. El enrutador que inicia la conexión es llamado cliente y se autentica ante el enrutador destino, de igual forma este último lo hace ante el enrutador cliente.

5. Administración de Usuarios de una VPN en W2K

Una gran ventaja que existe al utilizar W2K para la VPN es que permite tener el manejo y la organización de los usuarios de la VPN de manera centralizada mediante Active Directory (AD). AD no es más que un repositorio de dato bajo el estándar LDAP que permite la creación de una base de datos maestra centralizada en el controlador de

dominio de la organización donde se puede manejar usuarios, equipos y servicios dentro de una red.

6. Servidores de Nombres y Manejo de Direcciones IP en W2K

La creación de un túnel VPN incluye la asignación de una dirección IP al cliente de acceso remoto por parte del servidor VPN. Esta dirección o número IP le permite al cliente remoto poder identificarse una vez que el servidor VPN le concede acceso a la red privada. La asignación de ésta dirección se puede realizar de manera manual especificándole al servidor el rango de direcciones que puede otorgar o también puede realizarse mediante el servicio DHCP que forma parte del sistema operativo, y cuya función es la de asignar dinámicamente direcciones a los clientes que lo soliciten. El servicio DHCP también es utilizado para definir el servidor de nombres que se le será asignado (DNS) a los clientes remotos para una vez que formen parte de la red interna.

Para que un servidor VPN esté disponible a los usuario que deseen conectarse a él, se deben de cumplir dos condiciones principales: primero se tiene que asegurar que al servidor VPN se le sea asignado una dirección IP pública - en el caso en que la conexión VPN sea hecha en localidades geográficamente distintas- o una dirección alcanzable cuando este a lo interno de una organización. Como segunda condición aunque no es imprescindible se le tiene que asignar un nombre que al igual que la dirección pública sea visto y reconocido en la Internet de tal manera que sea más fácil aprenderse una palabra, que una serie de números.

7. Protocolos de Autenticación en W2K

W2K soporta una gran variedad de protocolos para la autenticación punto a punto, entre estos están:

- Password Authentication Protocol (PAP)
- Challenge – Handshake Authentication Protocol (CHAP)
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)
- MS-CHAP versión 2
- Extensible Authentication Protocol- Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol- Transport Level Protocol (EAP-TLS)

MS-CHAP y MS-CHAP v2 son protocolos de autenticación basados en passwords. EAP-TLS está diseñado para usarse en conjunto con una infraestructura de certificados. El cliente VPN envía su certificado de usuario para autenticarse y de igual forma lo hace el servidor VPN que envía un certificado de maquina para tal propósito. La utilización de Certificados Digitales es el método de autenticación más fuerte y no esta basado en passwords.

8. Mecanismos de Encriptación

W2K utiliza varios mecanismos de encriptación en una VPN. Estos están divididos en dependencia de su fortaleza.

- Encriptación Básica: MPPE 40 bits para PPTP y DES 56 bits para L2TP.
- Encriptación Fuerte: MPPE 56 bits para PPTP y DES 56 bits para L2TP.
- Encriptación Extra-Fuerte: MPPE 128 bits para PPTP y 3DES para L2TP.
- También se utiliza IPSEC como encriptación para L2TP

La utilización de estos depende del grado de seguridad que se desee, pero se ha de tomar en cuenta que se requiere de mayor capacidad de procesamiento en los servidores donde se implemente la VPN cuando se utilicen mecanismos de encriptación de gran fortaleza.

9. Protocolos de Túnel en W2K

W2K soporta la utilización de los protocolos de Túneles más reconocidos como los son PPTP y L2TP. El modulo RRAS para la creación de una VPN tiene la capacidad de manejar hasta 128 túneles PPTP y 128 Túneles L2TP.

9.1. Point to Point Tunneling Protocol (PPTP)

Las conexiones VPN basadas en PPTP proveen únicamente autenticación y encriptación a nivel de usuario.

- ✓ Autenticación de Usuarios con PPTP

El protocolo PPTP utiliza los mecanismos de autenticación basados en los protocolos de autenticación de usuario PPP, tales como EAP, MS-CHAP, CHAP y PAP. EAP-TLS utilizando MS-CHAP v2 es altamente recomendado ya que provee autenticación mutua y representan los métodos más seguros para el intercambio de credenciales.

- ✓ Encriptación con PPTP

PPTP utiliza MPPE para la encriptación, el cual hace uso del algoritmo RSA. MPEE sólo está disponible cuando se utiliza tanto EAP-TLS o MS-CHAP v1 ó v2. MPEE puede utilizar llaves de encriptación de 40, 56 y 128 bits según el nivel de seguridad que se requiera.

PPTP puede ser usado con una variedad de cliente de Microsoft incluyendo Win 95 (utilizando Windows Dial-UP Networking 1.3) Win98, Win Me, Win 2000 y Win XP.

Las conexiones VPN basadas en PPTP proveen confidencialidad de datos (los datos no pueden ser interpretado sin la correspondiente llave), sin embargo no proveen ni integridad de los datos ni mucho menos autenticación de datos.

9.2. Layer 2 Tunnelling Protocol (L2TP /IPSEC)

Las conexiones VPN basadas en L2TP a diferencia de las basadas en PPTP ofrecen autenticación de usuarios, autenticación mutua de computadoras, encriptación, autenticación e integridad de datos.

- ✓ Autenticación de Usuarios con L2TP/IPSEC

La autenticación de los clientes ocurre a dos diferentes niveles, primero es autenticada la computadora y luego es autenticado el usuario.

Autenticación de Computadora IPSEC: La autenticación mutua entre el cliente VPN y el Servidor VPN se lleva a cabo cuando se establece una Asociación de Seguridad (AS) IPSEC ESP a través de intercambio de certificados. Es por esa razón que para usar

L2TP/IPSEC es necesario que se instalen certificados tanto en e cliente VPN como en el Servidor.

Autenticación de Usuario L2TP: El cliente que intenta realizar una conexión L2TP es autenticado utilizando los protocolos de autenticación de usuario basados en PPP tales como EAP, MS-CHAP, CHAP.

- ✓ Encriptación con L2TP/IPSEC

Al utilizar L2TP/IPSEC la encriptación es determinada por el establecimiento de las AS de IPSEC. Los algoritmos de encriptación disponibles para esto son:

- DES con una llave de 56 bits.
- TRIPLE DES (3DES) la cual utiliza tres llaves de 56 bits y está diseñado para ambientes donde se requiera una alta seguridad.

- ✓ Autenticación e Integridad de Datos con L2TP/IPSEC

La autenticación e integridad de datos al utilizar L2TP/IPSEC es proporcionado por cualquiera de las dos opciones siguientes:

- Un Código de Autenticación del mensaje resumen (HMAC) (MD5), un algoritmo de resumen que produce un resumen de 128 bits de la carga autenticada.

- Un algoritmo de resumen seguro de HMAC (SHA), un algoritmo de resumen que produce un resumen de 60 bits de la carga autenticada.

La utilización de conexiones VPN basadas en L2TP utilizando IPSEC, provee confidencialidad, integridad, autenticación y no repudio, los cuatro elementos principales del concepto de Seguridad. Los clientes VPN basados en L2TP no pueden estar detrás de NAT porque IKE el protocolo que negocia las asociaciones de seguridad (As) de IPSEC, y el tráfico protegido IPSEC son incompatibles con NAT.

10. Infraestructura AAA en W2K

En Windows 2000 Server una infraestructura AAA es la encargada de garantizar:

- La autenticación de las credenciales de los clientes VPN.
- La autorización de la Conexión VPN.
- La elaboración de registros sobre la creación y finalización de conexiónes VPN.

Se conoce como infraestructura AAA por sus siglas A: Authentication, A: Authorization, A: Accounting. En un Servidor VPN el proceso de autenticación y registro puede ser configurado para ser realizada por WINDOWS o RADIUS (Remote Authentication Dial-In User Service - Servicio de Acceso Telefónico de Autenticación Remota de usuario).

Cuando se configura Windows como el proveedor de autenticación, el servidor VPN lleva a cabo la autenticación de la conexión VPN comunicándose con un controlador de dominio utilizando un procedimiento de llamada remota segura llamada RPC, la autorización del intento de conexión se da a través de las propiedades de marcado del usuario y las políticas de acceso remoto local.

Por el otro lado cuando se configura RADIUS como el proveedor de autenticación, el servidor VPN delega al servidor RADIUS para que realice tanto la autenticación como la autorización. Cuando se intenta una conexión VPN, las credenciales del cliente y otros parámetros de conexión son usados para crear un mensaje de solicitud de acceso que es enviado al servidor RADIUS. Si el intento de conexión es exitoso, el servidor envía un mensaje de aceptación de acceso, por el contrario devuelve un mensaje de negación de acceso.

Los registros de las conexiones VPN son almacenadas por Windows en una ruta especifica basada en las configuraciones de destino de archivos locales. Si se utiliza RADIUS el servidor VPN envía mensajes de registros al correspondiente servidor quien se encarga de almacenarla.

11. Políticas de Acceso Remoto en W2K

Se entiende por políticas de acceso remoto a una serie de reglas que determinan si los intentos de conexión con el servidor son aceptados o rechazados. Para cada regla, existen una o más condiciones, configuraciones de perfiles y configuraciones de permiso de acceso remoto.

Cuando se realiza un intento de conexión, se evalúa el mismo utilizando las condiciones especificadas en las políticas. Si el intento de conexión no cumple con las condiciones establecidas, el intento de conexión se rechaza.

Si una conexión cumple con todas las condiciones de las políticas se le concede permiso y se define un perfil en el cual se especifica una serie de restricciones aplicadas a la conexión.

Las políticas de acceso remoto están conformadas por los siguientes elementos:

- Condiciones: son uno o más atributos que se comparan con la configuración del intento de conexión. Si existen múltiples condiciones, entonces todas deben de corresponder con la configuración del intento de conexión para que pueda cumplir con la política. En módulo RRAS de W2K están disponibles las siguientes condiciones:

  + Called-Station-Id: El cual especifica el número de teléfono marcado por el usuario.
  + Calling-Station-Id: Especifica el número de teléfono desde el cual se originó la llamada.
  + Client Friendly Name: Es el nombre descriptivo que se le asigna al cliente RADIUS.
  + Client Ip-Address: Dirección IP del Cliente RADIUS.
  + Client Vendor: Especifica el fabricante de Proxy o NAS RADIUS.
  + Day-and-Time Restrictions: Especifica los periodos de tiempo y días de la semana durante los cuales le es permitido al usuario conectarse.
  + Framed-Protocol: Protocolo que se usará.
  + NAS Identifier: Cadena que identifica el NAS que origina la Solicitud (Solo para IAS)
  + NAS IP Adress: Dirección IP del NAS que origina la solicitud (Solo para IAS).

- NAS-Port-Type: Especifica el tipo de puerto físico usado por el NAS que origina la solicitud.
- Service Type: Tipo de Servicio que el usuario ha solicitado.
- Túnel Type: Protocolo de Túnel que se utilizará.
- Windows Group: Grupos de Windows a los que pertenecen los usuarios.

- Permisos: Se utiliza la configuración de los permisos para ceder o negar el acceso remoto para el intento de conexión de los usuarios.

- Configuración de Perfiles: Un perfil de una política de acceso remoto no es más que un perfil de usuario que se aplica a una conexión cuando es autorizada. Podemos utilizar los siguientes perfiles de configuración:

RRAS permite configurar los siguientes perfiles:

a. Restricciones de Marcado

- Desconectar si esta inactivo más de un minuto.
- Limitar la longitud máxima de sesión.
- Restringir el marcado a los días y horas especificados.
- Restringir el marcado a un número específico.
- Restringir el medio de marcado.

b. IP

Mediante la cual se define la directiva de asignación de direcciones IP para enrutamiento y acceso remoto.

- Directivas de Asignación de direcciones IP.
- Definición de Filtros y Paquetes que se aplican a la conexión.

c. Configuración de Multi-Vínculo.

- Usar como predeterminada la configuración del servidor.
- Deshabilitar el Multi-Vínculo.

- Permitir Vínculo Múltiple.

d. Autenticación

En RRAS están disponibles los mecanismos de autenticación disponibles en W2K.

e. Cifrado

En RRAS están disponibles los mecanismos de encriptación disponibles en W2K.

B. Diseño

La etapa de diseño de una VPN, es la más importante porque de ella depende su adecuado funcionamiento. En esta etapa se especifican todos los detalles de configuración que se utilizarán cuando se implemente la VPN.

1. Tipo de Conexión VPN a Utilizar.

Como ya se mencionó anteriormente la creación de una VPN a través de W2K puede ser realizada a través de dos diferentes maneras: VPN de Acceso Remoto y VPN de Enrutador a Enrutador.

Es el presente estudio monográfico se utilizará una **VPN de Acceso Remoto** que permita acceso a los usuario del SNIP a la red de la SEJUVE, contribuyendo de esa forma la transmisión de información de manera segura y rápida. El servidor VPN estará ubicado en las instalaciones de la SEJUVE y estará configurado para permitir el acceso solo a las personas previamente identificadas.

Este tipo de implementación no sólo permite el acceso de los usuarios del SNIP a través de Internet sino que también permite a los mismos usuarios de la SEJUVE conectarse desde su casa y poder realizar las mismas tareas como si estuvieran físicamente en las instalaciones de la SEJUVE.

2. Infraestructura de Red Interna

Para la implementación de la VPN de acceso remoto utilizando W2K se utilizará una computadora con un procesador AMD ATHLON XP 2000 de 1.6 Ghz con 256 Mb de memoria Ram y un disco duro de 40 GB como servidor VPN. Este equipo poseerá dos interfaces o tarjetas de red, una conectada directamente a Internet y la otra conectada a una de las interfaces de la puerta de enlace (enrutador).

Cabe destacar que el servidor VPN será instalado de tal forma que no modifique en ningún sentido la infraestructura de red interna con que cuenta actualmente la SEJUVE. Mediante el siguiente gráfico se muestra un esquema de la ubicación del servidor VPN que permitirá el acceso hacia la red SEJUVE.

La ilustración III-1 muestra la ubicación que tendrá el servidor VPN en la SEJUVE y por medio de la cual se permitirá el acceso de usuarios remotos que tengan un certificado valido.

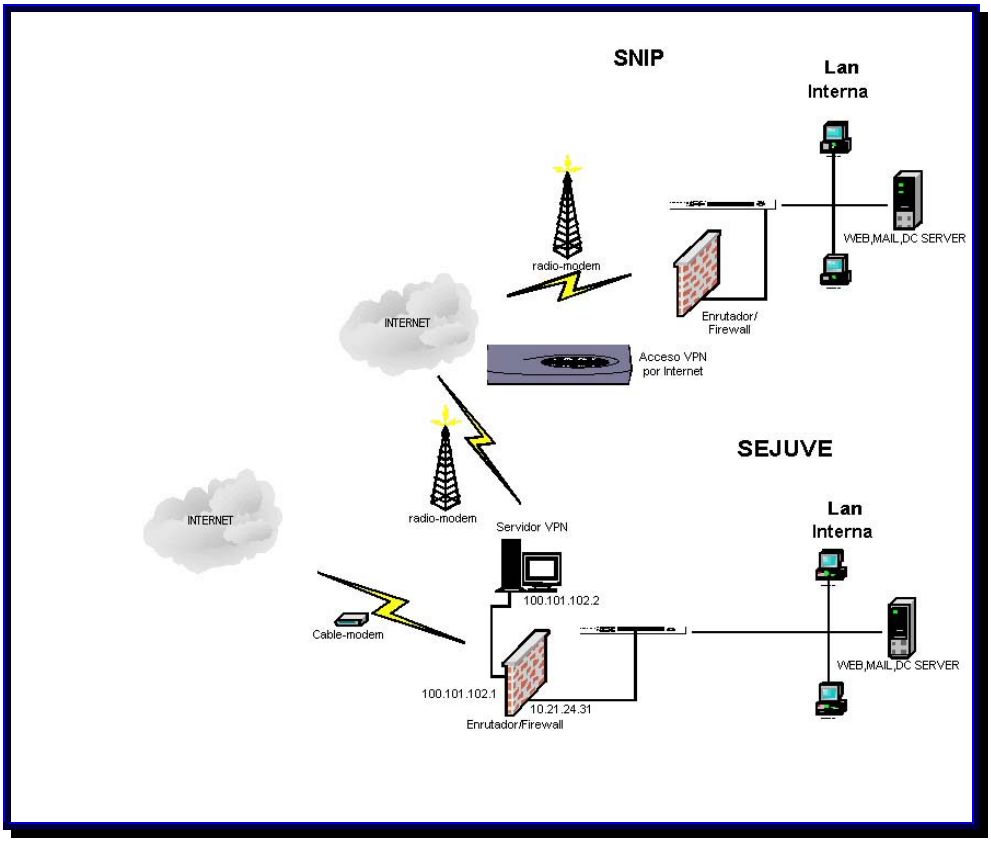


Ilustración III-1: Ubicación del Servidor VPN

Este servidor VPN estará conectado a una de las interfaces del enrutador de la SEJUVE, quien será el encargado de permitir el acceso a la red interna.

La configuración de la interfase interna del servidor VPN y la interfase del enrutador se configurarán de la siguiente manera:

a) Interfase dedicada a la red interna.

Dirección IP: **100.101.102.2**
Mascara de Subred: **255.255.254.0**.
Dirección de Gateway: **100.101.102.1**.
Nombre de Equipo: **VPN**
Servidor DNS: **10.21.24.30**

b) Interfase del enrutador a la cual se conecta el servidor VPN.

Dirección IP: **100.101.102.1**
Mascara de Subred: **255.255.254.0**.
Dirección de Gateway: **Default**.

3. Infraestructura de Internet.

a) Interfase dedicada a la conexión de Internet

Dirección IP: **165.98.154.16**
Mascara de Subred: **255.255.254.0**.
Dirección de Gateway: **165.98.154.1**.
Servidor DNS primario: **165.98.148.2**
Servidor DNS secundario: **216.6.48.5**

La dirección IP de la segunda interfase del servidor VPN es una dirección IP pública, asignada por el proveedor de Internet. El enlace a Internet para la creación del enlace PP por parte de la SEJUVE se debe de realizar utilizando tecnología de radio-modem como especifica el esquema o grafico mostrado anteriormente, pero debido a que esta tecnología no está presente en la SEJUVE y el autor de este estudio no tiene la

capacidad económica para poder adquirirla se utilizará una solución alternativa de cable-modem a una velocidad de 256 k.

El inconveniente con la dirección IP asignada por el proveedor es que está dada en números, y para muchas personas es difícil de recordarla, por lo que es importante asegurarse que el servidor VPN sea visible a través de un nombre específico que identifique a ese equipo. Con este propósito se registrara el nombre del servidor VPN en el servidor DNS de la SEJUVE, para que pueda ser accesado por medio de un nombre.

El servidor VPN estará disponible las 24 horas del día ya que se contará con un enlace a Internet de banda ancha el cual garantiza la disponibilidad permanente del servidor VPN y la eficiencia en la transmisión de información.

De igual forma los Clientes contaran con servicios de Internet (a través de la red del SNIP) de banda ancha que garantizará al igual que con el servidor no solo la capacidad para poder acceder en el momento que se desee, sino que también permitirá que la transferencia de información se realice de manera ágil.

4. Software para Servidor y Clientes

Como ya se describió anteriormente el software que se utilizará para el servidor VPN será W2K. Para los Clientes se utilizara Windows 2000 Pro y Windows XP, por ser estos los SO's para clientes que poseen mayores capacidades para la creación de túneles. Sin embargo queda abierta la posibilidad estos como son Win 98, Win Me etc., a través de la instalación de un componente adicional para manejo de túneles.

5. Seguridad

5.1. Protocolos de Túneles.

Como se describió en la fase de análisis, W2K tiene la capacidad de manejar dos protocolos de Túneles: L2TP y PPTP. PPTP es generalmente utilizado con autenticación basada en claves o passwords, por el contrario L2TP utiliza certificados digitales como método de autenticación. En este estudio se pretende utilizar certificados digitales para autenticar a los usuarios y equipos ante el servidor VPN por lo que se debe utilizar el protocolo L2TP. Al utilizar certificados digitales es necesaria la existencia de una

infraestructura de clave pública (PKI) que se haga cargo de la administración de los certificados utilizados para los usuarios de la VPN

En los anexos de este estudio se incluirá de manera rápida los pasos a seguir para la implementasen de una VPN utilizando PPTP, para que sirva a todas personas o instituciones que no requieran altos niveles de seguridad y que deseen tener acceso remoto a sus redes internas.

En este estudio el servidor VPN será configurado para poder crear 5 túneles L2TP y 5 PPTP de tal manera que se puedan utilizar 5 clientes o usuarios simultáneos conectados al servidor VPN.

5.2 Protocolos de Autenticación.

La utilización del protocolo L2TP como protocolo de túneles nos permite utilizar cualquier protocolo de autenticación de W2K ya que la autenticación ocurre después que el cliente y servidor VPN han establecido un canal seguro de comunicación conocido como Asociación de Seguridad de IPSEC, sin embargo es recomendable utilizar ya sea MS-CHAPv2 (con password) o EAP-TLS (con certificados) para proveer autenticación de usuario robusta. Para cumplir con el propósito de este estudio de autenticarse con certificados digitales se utilizara EAP-TLS.

5.3 Mecanismos de Encriptación.

La encriptación al utilizar el protocolo L2TP esta determinado por el establecimiento de las AS de IPSEC. En este estudio se utilizará el algoritmo de encriptación DES (Data Encription Standard) con una llave de 56 Bits que equivale a decir que es una encriptación básica.

6. Manejo de la Red Privada Virtual

a) Manejo de Usuarios

El manejo de usuarios en la VPN se va a realizar a través de una base maestra localizada en el controlador de dominio principal. La aplicación a cargo de esta realizar esta tarea será Active Directory modulo que forma parte de W2K.

b) Manejo de Direcciones y Servidores de Nombre.

El servidor VPN se debe encargar de otorgar una dirección IP virtual a cada cliente que se conecte a el. Para esto se debe configurar el servidor manualmente con el siguiente rango de direcciones estáticas y con el nombre del servidor DNS que los clientes deben conocer para poder ser parte de la red interna.

- Rango de Direcciones a Otorgar (10 Clientes):

100.101.102.3 - 100.101.102.12.

- Servidor DNS: 10.21.24.30

La ilustración III-2 muestra el modulo RRAS donde se le especifica al servidor VPN que otorgue a los clientes que se conecten a él un rango de direcciones pre-establecidas.

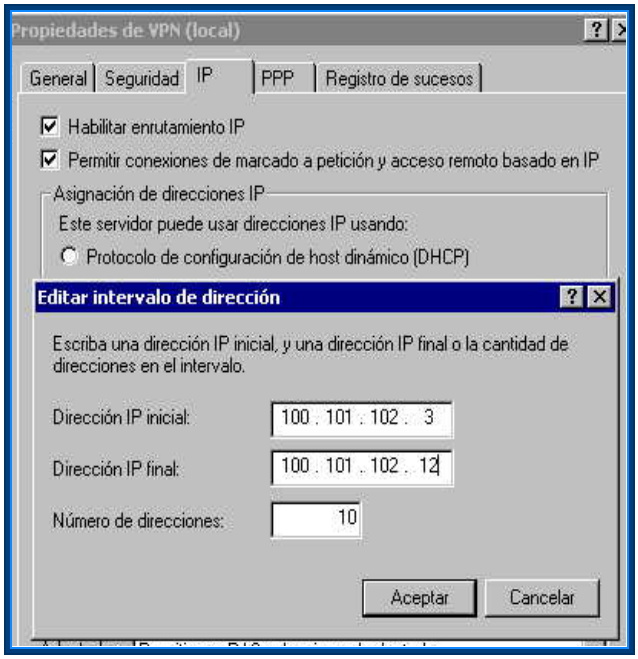


Ilustración III-2: Rango de Direcciones que el servidor VPN otorga.

c) Manejo de Acceso

El manejo del acceso de usuario a un servidor VPN se hace a través de las propiedades de marcado de los usuarios en Active Directory y en las políticas de acceso remoto. Para este estudio se pretende manejar el acceso en base a usuarios por lo que se debe seleccionar la opción Allow Access (Permitir Acceso) para que los usuarios que se especifiquen puedan conectarse.

7. Infraestructura AAA

Una infraestructura AAA en W2K puede ser configurado para utilizar RADIUS o el mismo Windows como el proveedor de autenticación y de registro. Para efectos de este estudio se utilizará Windows como proveedor de autenticación para autenticar las credenciales de los clientes VPN.

De igual forma se utilizará Windows como el proveedor de registros. Estos registros almacenan información sobre la actividad de las conexiones VPN que se realizan y son almacenadas por defectos en el archivo logfile.log en el directorio de sistema de Windows.

8. Políticas de Acceso Remoto.

a) Condiciones

En el presente estudio se utilizaran las siguientes condiciones:

- Day-and-Time Restrictions: Sin restricción de Horario.
- Túnel-Type: Configurado para utilizar el protocolo L2TP.

b) Permisos

- Grant Permission: Si está habilitado el permiso de acceso telefónico del usuario conceder permiso de acceso remoto.

c) Perfiles de Configuración

- Restricciones de Marcado: Sin ninguna restricción.
- IP: Las direcciones IP serán asignadas por el Servidor VPN, definidas manualmente.
- Los mecanismos de autenticación que se utilizarán serán MS-CHAP v2 y EAP-TLS para poder utilizar Certificados Digitales.
- El nivel de encriptación que se utilizara para la VPN será básico.

IV. Análisis, Diseño e Implementación de una PKI

IV. ANALISIS, DISEÑO E IMPLEMENTACION DE UNA PKI

Antes de poder implementar una VPN con certificados digitales como método de autenticación, es necesario la existencia de una infraestructura que se encargue del manejo y la administración de los mismos.

La siguiente sección tiene como propósito principal implementar la Infraestructura de Clave Pública (PKI) que se encargue de la gestión de todos los certificados necesarios para la VPN.

Una PKI permite a las aplicaciones cliente servidor (como la VPN) aumentar la confianza en las credenciales de autenticación entre ambos. Una PKI es un diseño estructural para establecer comunicación, mensajería y transacciones seguras sobre las redes apoyándose principalmente en la criptografía de llaves públicas y los certificados digitales.

No existe una metodología estandarizada para el desarrollo de una PKI, más bien cada proveedor o entidad utiliza una metodología propia cuando se necesita hacer uso de ella. Después de hacer un análisis de varias metodologías, como la de la compañía Baltimore y la de la Compañía Microsoft, se decidió hacer uso de una metodología que incluya los mejores elementos de cada una de ellas e implementarla en este estudio. Esta metodología para la utilización de una PKI, está compuesta de 3 fases principales:

a) Análisis: Fase que tiene como propósito describir de manera breve todas las características del software que se utilice para desarrollar la PKI, así como identificar los requerimientos de certificación necesarios para que la cumpla adecuadamente con su objetivo.

b) Diseño: En esta fase se diseña la PKI basada en los requerimientos descritos en la fase anterior. Se identifican los componentes de Software y Hardware que se utilizarán y se detallan sus respectivas configuraciones.

c) Implementación: Esta fase consiste en llevar a cabo el diseño de la PKI, instalando, configurando y probando tanto el hardware y software que se utilice.

A. Análisis

Una PKI puede manejar certificados digitales de autenticación no sólo para una VPN, también y muy comúnmente en estos días se emiten certificados para transacciones electrónicas e incluso correo electrónico. Grandes compañías como Verisign y Twatwe, se dedican actualmente a este negocio.

A pesar de que estas compañías son reconocidas a nivel mundial por ser las lideres en el campo, los costos de adquisición de un certificado pueden ser altos si se piensa que se tiene que emitir uno para cada usuario que utilice la tecnología que se propone. Otro inconveniente es que toda la infraestructura de manejo de estos certificados es realizada por la misma compañía limitando el acceso de parte de los usuarios al manejo de los mismos.

Pero actualmente este problema está siendo superado dada la oportunidad que una organización tiene de poder implementar su propia infraestructura de certificados (PKI) para los fines que estime conveniente, facilitándole de esa manera tener un control absoluto sobre la misma.

Existen varias soluciones en el mercado para que una organización pueda crear su propia PKI. En este estudio se utilizará W2K a través de los servicios de Servidor de Certificados y Active Directory por las siguientes razones:

a. Por ser W2K la plataforma para la creación de la VPN, lo cual facilita la interoperabilidad del servidor VPN con la PKI.

b. Por ser esta opción, la más conveniente al no tener que implementar software adicional.

c. Por estar basado en estándares del mercado, que facilita la interoperabilidad con terceros.

d. Debido a que la herramienta Servidor de Certificado es fácil de usar y administrar.

1. Componentes de una PKI en Windows 2000 Server.

El servidor de certificados de W2K como cualquier otra solución disponible basa su funcionamiento en una arquitectura. Esta arquitectura a su vez posee una serie de componentes que interactúan entre si para poder alcanzar el objetivo final, es decir la emisión de los certificados.

La Infraestructura de clave pública de Windows 2000 está formada por los siguientes componentes:

1.1. Las aplicaciones y servicios habilitados mediante clave pública.

Se trata de IIS, IPSec, inicio de sesión mediante tarjeta inteligente, EFS , Internet Explorer, Outlook y Outlook Express. Estos componentes interactúan entre ellos y utilizan los servicios de seguridad criptográfica. Algunos de ellos también realizan una administración de claves. Se basan todos en los estándares y pueden interoperar con entidades que no sean Microsoft. Obtienen las claves o certificados que necesitan de su propio almacén de usuario o de host, Active Directory y Exchange.

1.2. Servicios de Microsoft Certificate Server

Los Servicios de Microsoft Certificate Server constituyen el servicio de emisión de certificados. Su trabajo consiste en aceptar solicitudes de certificados, emitir certificados y publicar la lista de revocación de certificados.

Hay dos tipos de entidades emisoras de certificados de Microsoft: de empresa e independiente. Una entidad emisoras de certificados de empresa tiene como tarea emitir certificados a usuarios y equipos de dominio de acuerdo con algunas políticas de acceso establecidas. Una entidad emisora de certificados independiente tiene como tarea emitir certificados a entidades fuera de los dominios de Windows 2000, como clientes y usuarios de otras organizaciones.

Algunas de las diferencias entre las dos entidades emisoras de certificados son evidentes por el modo en que funcionan sus módulos de directiva y de salida. Por ejemplo, puede que se defina una directiva que emita certificados automáticamente según determinadas reglas.

Como las entidades emisoras de certificados independientes pueden emitir certificados a cualquier tipo de entidad, incluso a entidades que no sean Windows 2000, son más apropiados para convertirse en sus entidades emisoras de certificados raíz. Pueden funcionar sin conexión, ya que no necesitan autenticar automáticamente a los solicitantes a diferencia de las entidades emisoras de certificados de empresa.

Los servicios de servidor de certificado en W2K permiten la utilización de más de una entidad certificadora para emitir certificados para diferentes propósitos, creando de esa manera una jerarquía. La entidad que se encuentra en el primer nivel de esa Jerarquía es conocida como raíz y tienen como propósito principal emitir certificados a entidades subordinadas. De igual forma estas entidades subordinadas pueden emitir certificados para otras entidades subordinadas (llamadas emisoras) o comportarse ellas mismas como emisoras y emitir certificados para usuarios y equipos finales. Tanto las entidades raíz como las subordinadas y emisoras pueden ser de empresa o independiente.

1.3. Plantillas de Certificados

Las plantillas son perfiles que definen el contenido de los certificados emitidos por las entidades emisoras de certificados de empresa de Microsoft. Este contenido incluye información de usuario como el nombre y la dirección de correo electrónico obtenida de Active Directory, la fecha de caducidad y la utilización prevista del certificado.

Cada plantilla está definida según su uso previsto. Por ejemplo, la plantilla de usuario denominada "Usuario" permite a su titular utilizar EFS, cifrar correo electrónico, firmar correo electrónico y autenticarse a sí mismo en los servidores Web. La plantilla de equipo denominada "WebServer" permite a su titular autenticarse a sí mismo en los exploradores Web. La Tabla IV-1 ofrece una lista de plantillas que manejan las entidades certificadoras de empresa.

Tabla IV-1: Plantillas de Certificados.

Nombre de la plantilla de certificado	Finalidad del certificado	Emitido a usuarios o equipos
Administrador	Firma de código, firma de lista de confianza de certificados (CTL), EFS, correo electrónico seguro, autenticación de clientes	Usuarios
Sesión autenticada	Autenticación de clientes	Usuarios
EFS básico	EFS	Usuarios
Equipo	Autenticación de clientes, autenticación del servidor	Equipo
Firma de código	Firma de código	Usuarios
Controlador de dominio	Autenticación de clientes, autenticación del servidor	Equipos
Agente de recuperación EFS	Recuperación de archivos	Usuarios
Agente de inscripción	Agente de solicitud de certificados	Usuarios
Agente de inscripción (solicitud sin conexión)	Agente de solicitud de certificados	Usuarios
IPSec (solicitud sin conexión)	Seguridad del Protocolo de Internet	Equipos
IPSec	Seguridad del Protocolo de Internet	Equipos
Enrutador (solicitud sin conexión)	Autenticación de clientes	Equipos/enrutadores
Inicio de sesión con tarjeta inteligente	Autenticación de clientes	Usuarios
Usuario de tarjeta inteligente	Autenticación de clientes, correo electrónico seguro	Usuarios
Entidad emisora de certificados subordinada	Todos	Equipos
Firma de la lista de confianza	Firma de la lista de certificados de confianza	Usuarios
Usuario	EFS, correo electrónico seguro, autenticación de clientes	Usuarios
Firma de usuario únicamente	Correo electrónico seguro, autenticación de clientes	Usuarios
Servidor Web	Autenticación del servidor	Equipos

.

1.4. Módulo de Directiva

La entidad emisora de certificados llama al módulo de directiva para decidir si un certificado debería emitirse, denegarse o marcarse como pendiente para que el administrador de la entidad emisora de certificados lo revise.

En una entidad emisora de certificados de empresa, el módulo proporcionado con Windows 2000 aceptará solicitudes de certificados de los usuarios con acceso de lectura y de registro a la entidad emisora de certificados. La característica definitoria de una entidad emisora de certificados de empresa es que autentica a las entidades solicitantes utilizando las cuentas de dominio de estas últimas. De manera predeterminada, todos los usuarios autenticados tienen un acceso de este tipo.

El módulo comprobará a continuación que la plantilla que se ha solicitado se encuentra realmente disponible para ser emitida por parte de la entidad emisora de certificados y, posteriormente, comprobar que el usuario tiene acceso de registro a la plantilla.

En una entidad emisora de certificados independiente, el módulo de directiva aceptará solicitudes de los usuarios con acceso similar a la entidad emisora de certificados, que de manera predeterminada estén autenticados o no. Posteriormente marcará las solicitudes como pendientes de manera predeterminada, o también puede configurarlo para que las emita automáticamente. Las plantillas no se definen para entidades emisoras de certificados independientes.

En ambos tipos de entidades emisoras de certificados, el módulo también agregará dos extensiones X.509v3 al certificado con los siguientes elementos:

- ✧ **Registros del punto de distribución de listas de revocación de certificados (CDP).** Estos señalan dónde la entidad emisora de certificados publica su lista de revocación de certificados.
- ✧ **Registros de acceso de información de autoridad (AIA).** Estos señalan dónde se publica el certificado de la entidad emisora de certificados.

Estos señaladores adoptan la forma de una dirección URL y pueden señalar Active Directory (LDAP), la interfaz Web de la entidad emisora de certificados (http) o la carpeta compartida de la entidad emisora de certificados (archivo), si alguna se especifica

durante la instalación. Cuando se forman estas direcciones URL, se debe utilizar la sintaxis de parámetros reemplazables mostrada en la siguiente tabla.

Tabla IV-2: Parámetros reemplazables de la entidad emisora de certifcados.

Variable	Valor
%1	Nombre DNS del servidor de la entidad emisora de certificados
%2	Nombre NetBIOS del servidor de la entidad emisora de certificados
%3	Nombre de la entidad emisora de certificados
%4	Extensión de renovación de la entidad emisora de certificados
%5	Ubicación de la raíz de dominio de Active Directory
%6	Ubicación del contenedor de configuración de Active Directory
%7	El nombre "aséptico[rdquo] de la entidad emisora de certificados, truncado a 32 caracteres con un guión al final

1.5. Módulo de Salida

La entidad emisora de certificados llama al módulo de salida una vez ha emitido un certificado. La tarea del módulo es publicar el certificado en la ubicación especificada en la solicitud de certificado, generalmente Active Directory para las entidades emisoras de certificados de empresa y el sistema de archivos para las entidades emisoras de certificados independientes. El módulo es también responsable de publicar la lista de revocación de certificados o CRL (Certificate Revocation List).

1.6. Complemento Entidad emisora de certificados o MMC

El complemento Entidad emisora de certificados, permite ver y administrar certificados y solicitudes, configurar la entidad emisora de certificados y publicar manualmente la lista de revocación de certificados de la entidad emisora de certificados.

Este complemento permite realizar lo siguiente:

- Ver los certificados revocados y publicar manualmente la lista de revocación de certificados.
- Ver y revocar los certificados emitidos.
- Ver, emitir y denegar cualquier solicitud pendiente. Este tipo de solicitudes sólo es posible en entidades emisoras de certificados independientes.

- Ver solicitudes fallidas. Las solicitudes pueden quedar anuladas por el módulo de directiva si el solicitante no está autorizado a registrarse en la lista de control de acceso de la entidad emisora de certificados o por el Administrador de la entidad emisora de certificados que revisa las solicitudes pendientes.
- Para las entidades emisoras de certificados de empresa solamente: ver, agregar y quitar Opciones de directiva (las plantillas de certificados) que la entidad emisora de certificados puede emitir. Puede especificar a qué entidades pueden emitirse qué plantillas de certificados en Active Directory.

1.7. Complemento de Certificados o MMC

Este complemento puede ser utilizado para la administración de los certificados tanto de usuario, equipo como de servicios. Mediante este complemento se pueden realizar las siguientes tareas:

- Solicitar un certificado por medio del asistente de solicitud de Certificados.
- Almacenar los certificados de las Entidades Emisoras raíz de Confianza.
- Almacenar los certificados de las Entidades Emisoras subordinadas o intermedias.
- Administración de los certificados en los que se confían.
- Almacenar los certificados de las Entidades Emisoras de Terceros.

1.8. Ciclos de vida de los certificados

Un par de claves pública-privada de una entidad puede considerarse como otra credencial para autenticarse ante un controlador de dominio además de la contraseña de Windows. Dado que la clave privada de una entidad no se comparte con nadie más, posee requisitos de generación y de almacenamiento diferentes que una contraseña de Windows. Asimismo, la clave pública tiene requisitos de certificación (autenticación) y de publicación exclusivos.

2. Claves de Usuario

2.1. Generación y certificación

La generación y certificación de claves sucede conjuntamente y, por lo general, estos procesos los inicia un usuario que solicita un certificado de una entidad emisora de

certificados. El usuario genera las claves utilizando uno de los proveedores de servicios criptográficos disponibles en su sistema.

2.2. Almacenamiento

La clave privada la administra un proveedor de servicios criptográficos y se almacena en el perfil del usuario o en una tarjeta inteligente. Con la protección robusta habilitada, se puede cifrar la clave con una contraseña que se debe introducirse cada vez que una aplicación necesite la clave. Una clave privada almacenada en una tarjeta inteligente está protegida por un PIN y por las propiedades físicas de la tarjeta inteligente.

La clave pública está empaquetada en el certificado y también se almacena en el perfil del usuario. Las entidades emisoras de certificados de empresa publicarán algunos tipos de certificados en Active Directory de manera predeterminada.

También se puede importar y exportar pares de claves. Se puede marcar las claves privadas como exportables durante la generación o cuando se importen. La exportación de certificados admite los formatos estándares DER X.509, CER X.509 y PKCS #7. PKCS #12 se utiliza cuando la clave privada se exporta junto con el certificado.

2.3. Publicación

Una entidad emisora de certificados de empresa pública automáticamente algunos tipos de certificados en Active Directory. Una entidad emisora de certificados independiente no publicará por lo general el certificado si se solicita utilizando los métodos descritos anteriormente.

2.4. Revocación

La entidad emisora de certificados puede revocar los certificados que emite por las siguientes razones:

- ✧ El usuario cambia su nombre.
- ✧ La clave privada del usuario se ha puesto en peligro; el usuario se registrará de nuevo para solicitar otro certificado con un par de claves nuevo.
- ✧ La clave de firma del usuario se ha puesto en peligro. Si otras partes pueden ahora emitir certificados en nombre del emisor, todos los certificados emitidos pierden su validez.

✧ El usuario abandona la organización o la parte de la organización que se encuentra bajo la responsabilidad de la entidad emisora de certificados.

✧ El propietario informático del certificado (los propietarios informáticos también pueden tener claves) ha sido sustituido, se ha puesto en peligro o ha sido retirado del servicio.

Técnicamente, la revocación se realiza publicando el número de serie del certificado en una lista de revocación de certificados firmada por la entidad emisora de certificados. Un certificado de una autoridad emisora se revoca si su clave privada se ha puesto en peligro, ya que ahora otras partes pueden emitir certificados en su nombre. Por lo tanto, todos sus certificados, incluso los emitidos a entidades emisoras de certificados subordinadas y los certificados emitidos por éstas, también se consideran revocados.

2.5. Renovación

Los usuarios pueden renovar sus certificados antes o después de su vencimiento. Pueden optar por mantener los pares de claves existentes o generar uno nuevo.

3. Claves de Host

Los usuarios con privilegios administrativos locales pueden administrar pares de claves de host utilizando el complemento Certificados.

3.1. Generación y certificación

Se puede invocar la solicitud de certificado en el complemento o en la interfaz Web de una entidad emisora de certificados, donde se tendrá que seleccionar la opción almacén del equipo local.

3.2. Almacenamiento

El almacén de claves del equipo almacena la clave privada. Las claves privadas no suelen protegerse, dado que los servicios que las utilizan se ejecutan en modo desatendido, sin la intervención del usuario.

3.3. Publicación

Las claves de host se publican del mismo modo que las claves de usuario.

3.4. Renovación

Se puede realizar la renovación manualmente, del mismo modo que con las claves de usuarios, o automáticamente, si se especifica en las directivas de clave pública.

3.5. Directivas de clave pública

Las directivas de seguridad de clave pública se definen en los objetos directiva de grupo y en el objeto directiva local. Estas directivas se tratan de directivas de equipo; por lo tanto, solamente se puede definir qué equipos, pero no qué usuarios, las recibirán dentro dominio o unidad organizativa.

Dentro de las directivas de clave pública tenemos las siguientes:

- **Directiva de opciones de solicitud automática de certificados.** Esta directiva define si los equipos deberían registrarse automáticamente para obtener certificados y con qué entidades emisoras de certificados de empresa deberían ponerse en contacto.
- **Entidades emisoras de certificados raíz de confianza y directivas de confianza de empresa.** Estas directivas definen lo siguiente:

  ' En qué entidades emisoras de certificados raíz pueden confiar los usuarios cuando comprueban certificados.
  ' Si los usuarios pueden confiar en entidades emisoras de certificados adicionales de su propia elección.
  ' El uso de claves en los certificados emitidos por todas esas entidades emisoras de certificados (las finalidades para las que estos certificados son válidos).
  ' Las entidades emisoras de certificados de Microsoft dentro del bosque de dominios se agregan automáticamente a estas directivas.

Para distribuir el certificado de las entidades emisoras de certificados que pertenecen a otras organizaciones o entidades emisoras de certificados comerciales, se utiliza la directiva de confianza de empresas. Esta directiva contiene listas de confianza de certificados (CTL), que son listas de certificados firmados digitalmente y usos permitidos de las claves. Para poder elaborar una se necesita un certificado de firma de lista de confianza de una entidad emisora de certificados de empresa.

- **Directiva de agentes de recuperación de datos encriptados.** No se trata realmente de una directiva de clave pública; es una directiva acerca de EFS. EFS define si hay una directiva de recuperación de datos encriptados dentro del alcance del objeto directiva. Si se define una directiva de recuperación, se rellena con los certificados de los agentes de recuperación.

3.6. Active Directory

Active Directory de W2K posee las siguientes propiedades:

- Se utiliza como un punto de publicación para certificados emitidos, certificados de entidades emisoras de certificados y listas de revocación de certificados.
- Almacena las Plantillas de certificados utilizadas por las entidades emisoras de certificados de empresa.
- Define qué Directivas de grupo son exigibles en los dominios, parte de las cuales son las directivas de clave pública.
- Se puede utilizar para asignar certificados a usuarios. Esta asignación se utiliza principalmente cuando los usuarios se autentican a sí mismos en IIS utilizando un certificado.

4. Proveedores de Servicios Criptográficos.

El servicio de servidor de certificado de W2K ofrece la siguiente lista de proveedores de Servicios Criptográfico, los cuales utiliza para la generación de la llave privada y su correspondiente clave pública.

- Gemplus Gemsafe Card CSP v 1.0
- Infineon Sicrypt BaseSmart Card CSP
- Microsoft Base CSP v 1.0
- Microsoft Enhanced CSP v 1.0
- Microsoft Strong CSP v 1.0
- Schlumberger Cryptographic Service Provider
- Microsoft Base DSS CP
- Microsoft Exchange CSP v 1.0
- Microsoft RSA Schannel CSP
- Microsoft Base DSS and DH CSP
- Microsoft Enhanced DSS and DH CSP

- Microsoft DH Schannel CPS
- Microsoft Enhanced RSA and AES CPS

4.1. Longitudes de Claves disponibles en W2K.

→ 512 Bits
→ 1204 Bits
→ 2048 Bits
→ 4096 Bits

4.2. Estándares de Cifrado de Clave Pública en W2K.

PKCS # 7: Estándar de sintaxis de mensajes encriptados, la base para las extensiones multipropósitos de correo de Internet Seguro (S/MIME). Define el formato para los mensajes firmados y encriptados.

PKCS # 10: Peticiones de Certificados. Usado por los clientes para solicitar los certificados de Autoridad Certificadora (CA- Certificate Authority).

PKCS # 11: Interfaz de elementos de cifrado. Similar a la CryptoAPI de Microsoft.

PKCS # 12: Intercambio de información personal (PFX). Habilita la transferencia cifrada de un equipo a otro de claves privadas y certificados asociados.

4.3. Aplicaciones y servicios habilitados mediante Clave Pública.

Las aplicaciones que se habilitarán para el uso de certificados digitales serán:
- Autenticación Cliente/Servidor (VPN utilizando L2TP).
- Firma Digital.
- Agente de Inscripción.

4.4. Cantidad necesaria de Entidades Certificadoras.

Para la certificación de las aplicaciones que se habilitaran mediante clave pública se necesitan como minino tres (3) autoridades certificadoras. Una autoridad

certificadora principal, una que se encargue de emitir certificados a los usuarios o equipos miembros del dominio principal y una última que se encargue de emitir a los equipos y usuarios no miembros del dominio principal.

Los requerimientos mínimos que deben poseer los equipos para llevar a cabo esta configuración se describen a continuación:

Para la AC Raíz de Empresa.

- Procesador XEON.
- Memoria RAM 512 Mb.
- 1 Disco Duro 30 GB Ultra-Sci.
- Sistema Operativo: Windows 2000 Server.

Para la AC subordinada de Empresa.

- Procesador de 1.2 Mhz o superior.
- Memoria RAM 256 Mb.
- Disco Duro de 40 GB IDE
- Sistema Operativo: Windows 2000 Server.

Para la AC subordinada Independiente.

- Procesador de 1.2 Mhz o superior.
- Memoria RAM 256 Mb.
- Disco Duro de 40 GB IDE
- Sistema Operativo: Windows 2000 Server.

a) Requerimientos de Usuarios.

Los usuarios que harán uso de los certificados son usuarios no experimentados, por lo que necesitan un sistema lo más transparente posible. Para lograr esa transparencia se requiere de una PKI (Infraestructura de Clave Pública), que ofrezca a los usuarios la capacidad para poder obtener los certificados y claves a través de una interfaz Web (en línea) o una variante fuera de línea para cuando la primera no esté disponible.

b) Requerimientos de Certificación.

Los requerimientos de certificación están conformados por los siguientes componentes:

+ Usuarios de los Certificados: Los usuarios que harán uso de los certificados serán: cada usuario con permiso para conectarse al servidor VPN, un usuario administrador encargado de solicitar certificados para aquellos clientes que no sean miembros del dominio principal.

+ Equipos que harán uso de los Certificados: Los equipos que utilizarán los certificados serán: cada cliente VPN, el servidor VPN, la AC raíz y las AC subordinada según se requiera.

+ Tipos de Certificados que se necesitan:

La tabla IV-3 muestra los tipo de certificados que se utilizarán en este estudio.

Tabla IV-3: Tipos de Certificados.

Tipo de Certificado	Propósito
Certificado de Usuario.	Probar la identidad del Usuario
Certificado de Administrador	Firma, Creación de Lista de Certificados de Confianza.
Certificado de Equipo	Probar la identidad del Cliente VPN
Certificado de Equipo	Probar la identidad del Servidor VPN
Certificado EFS	Inscripción de Certificados de otros Usuarios.
Certificado de AC raíz	Certificado de Autoridad Certificadora
Certificado de AC subordinada	Certificado de Autoridad Certificadora

c) Requerimientos de Seguridad para los Certificados.

+ Longitud de las Llaves Privadas.

- La longitud mínima para Llaves Privadas de Usuarios 512 bits.
- La longitud mínima para Llaves Privadas de administrador 1024 bits.
- La longitud mínima para Llaves Privadas para EFS 512 bits.
- La longitud mínima para Llaves Privadas del cliente VPN 1024 bits.
- La longitud mínima para Llaves Privadas del servidor VPN 1024 bits
- La longitud mínima para Llaves Privadas de AC raíz 2048 bits.
- La longitud mínima para Llaves Privadas para AC Subordinadas 1024 bits.

+ Algoritmos Criptográficos permitidos con los Certificados.

- Proveedor de Servicios Criptográficos (CSP):

  - Microsoft Base CSP v 1.0
  - Microsoft Enhanced CSP v 1.0
  - Microsoft RSA Schannel CSP.

- Algoritmos Criptográficos Permitido: Algoritmo de Llave Pública RSA en las longitudes 512,1024 bits y 2048.

+ Ciclo de Vida mínimo de los Certificados.

- Ciclo de Vida del Certificado de la AC raíz: 5 Años.
- Ciclo de Vida del Certificado de la AC subordinadas: 3 años.
- Ciclo de Vida del Certificado para el servidor VPN: 1.5 años
- Ciclo de Vida del Certificado para el cliente VPN: 1 año
- Ciclo de Vida del Certificado de usuarios: 4 y 8 meses.

+ Almacén de la Clave Privada.

La Clave Privada debe ser almacenada como mínimo en el perfil del usuario dueño de esa llave. La Clave Privada tiene que poder exportarse de tal manera que se pueda almacenar en dispositivos de almacenamientos más seguros como CD-R o cintas magnéticas.

B. Diseño

Como se describió al inicio, el diseño de la PKI utilizando el producto que se seleccionó (Windows 2000) se basa principalmente en los requerimientos que se plantearon en el análisis. La fase de diseño consta de las siguientes etapas:

1. Jerarquía de Certificación.

Para la emisión de los certificados que se utilizaran en la autenticación de los clientes ante el servidor VPN se utilizaran 3 entidades o autoridades certificadoras, las cuales se detallan a continuación.

1.1. Autoridad Certificadora Raíz de Empresa.

- Nombre: sejuve.gob.ni
- Dirección ip: 10.21.24.30
- Nombre de la máquina: server1
- Función: Emitir certificados para las autoridades certificadoras subordinadas.
- Tipo de Certificado: Certificado de Autoridad Certificadora autofirmado.
- Nivel en la jerarquía: Primer nivel.
- Tipo: Raíz de Empresa.
- Ubicación: Ubicada en el servidor principal o DC de la red SEJUVE.
- Longitud de la Clave Privada y Pública: 2048
- Algoritmo Utilizado: RSA
- Validez del Certificado: 5 años
- Almacenamiento de la Clave Privada: Local exportable
- Publicación de la Clave Pública y Certificado: Active Directory.

1.2. Autoridad Certificadora subordinada de empresa.

- Nombre: acsubem.sejuve.gob.ni
- Dirección IP: 10.21.24.92
- Nombre del equipo: acsubem.

- Función: Emitir certificados para los usuario y equipos miembros del dominio principal.
- Tipo de Certificado: Certificado de Autoridad Certificadora.
- Nivel en la jerarquía: Segundo nivel.
- Tipo: Subordinada de Empresa.
- Ubicación: Forma parte de la red interna de la SEJUVE como servidor miembro.
- Nombre del equipo en la que se instala: acsubem
- Longitud de la Clave Privada y Pública: 1024
- Algoritmo Utilizado: RSA
- Validez del Certificado: 3 años
- Almacenamiento de la Clave Privada: Local exportable
- Publicación de la Clave Pública y Certificado: Active Directory

1.3. Autoridad Certificadora subordinada Independiente

- Nombre: acsbind.sejuve.gob.ni
- Dirección IP: 10.21.24.93
- Nombre del equipo: acsubind
- Función: Emitir certificados para los usuario y equipos no miembros del dominio principal.
- Tipo de Certificado: Certificado de Autoridad Certificadora.
- Nivel en la jerarquía: Segundo nivel.
- Tipo: Subordinada Independiente.
- Ubicación: Forma parte de la red interna de la SEJUVE como servidor miembro.
- Nombre del equipo en la que se instala: acsubind
- Longitud de la Clave Privada y Pública: 1024
- Algoritmo Utilizado: RSA
- Validez del Certificado: 3 años
- Almacenamiento de la Clave Privada: Local exportable
- Publicación de la Clave Pública y Certificado: Active Directory.

La siguiente ilustración muestra la Jerarquía de autoridades certificadoras con las que se trabajará.

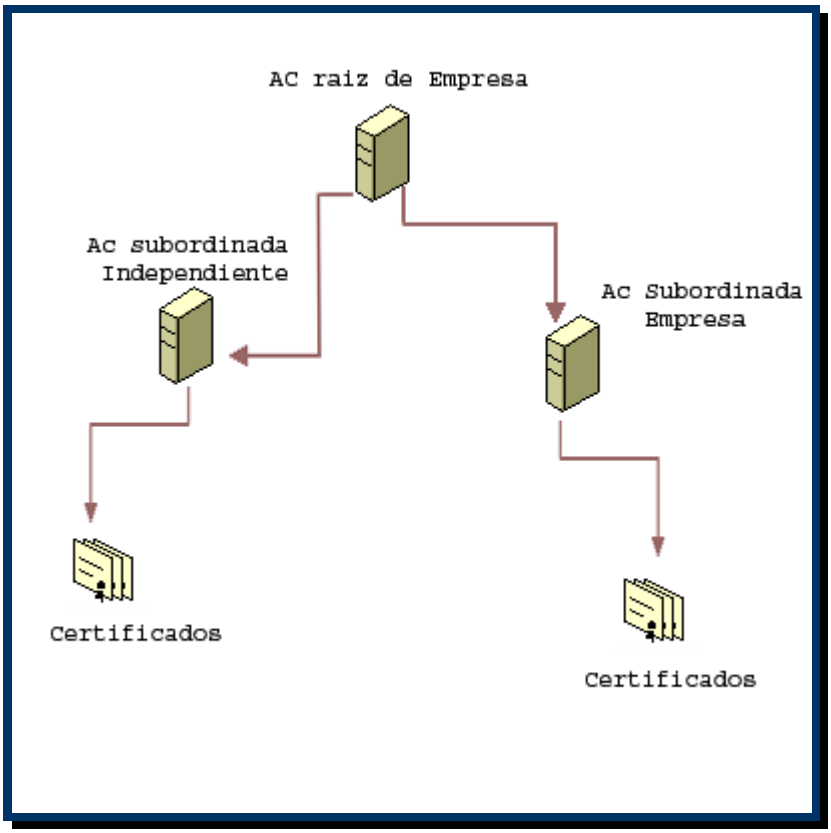


Ilustración IV-1: Jerarquías de Autoridades Certificadas.

2. Tipos de Certificados a emitir para usuario y Equipos.

Equipo: Servidor VPN
Tipo de Certificado: Equipo
Propósito: Autenticación de Servidor VPN

Equipo: Cliente VPN
Tipo de Certificado: Equipo
Propósito: Autenticación de cliente VPN

Usuario: Administrador
Tipo de Certificado: administrador
Propósito: Firma Digital, Firma las listas de certificados de confianza, autenticación de clientes.

Usuario: Administrador
Tipo de Certificado: EFS
Propósito: Inscripción de certificados para usuarios o equipos no miembros del DC

Usuario: Usuario Externo
Tipo de Certificado: Usuario
Propósito: Autenticación de usuario externo

3. Aspectos de Seguridad para los certificados de Usuario y Equipos.

Equipo: Servidor VPN
Longitud de Claves: 1024
Algoritmo Utilizado: RSA
Algoritmo Hash: SHA-1
CSP Utilizado: Microsoft RSA Schannel CSP
Validez del Certificado: 1.5 años
Almacenamiento de la Clave Privada: Almacenamiento Local pero exportable.
Publicación del Certificado y Clave Pública: Active Directory.

Equipo: Cliente VPN
Longitud de Claves: 1024
Algoritmo Utilizado: RSA
Algoritmo Hash: SHA-1
CSP Utilizado: Microsoft RSA Schannel CSP
Validez del Certificado: 1 años
Almacenamiento de la Clave Privada: Almacenamiento Local
Publicación del Certificado y Clave Pública: Active Directory.

Usuario: Administrador
Longitud de Claves: 1024
Algoritmo Utilizado: RSA
Algoritmo Hash: SHA-1
CSP Utilizado: Microsoft Enhanced CSP v 1.0
Validez del Certificado: 8 meses
Almacenamiento de la Clave Privada: Almacenamiento Local

Publicación del Certificado y Clave Pública: Active Directory.

Usuario: Administrador-EFS
Longitud de Claves: 512
Algoritmo Utilizado: RSA
Algoritmo Hash: SHA-1
CSP Utilizado: Microsoft Enhanced CSP v 1.0
Validez del Certificado: 8 meses
Almacenamiento de la Clave Privada: Almacenamiento Local
Publicación del Certificado y Clave Pública: Active Directory.

Usuario: Usuario Externo
Longitud de Claves: 1024
Algoritmo Utilizado: RSA
Algoritmo Hash: SHA-1
CSP Utilizado: Microsoft Enhanced CSP v 1.0
Validez del Certificado: 4 meses
Almacenamiento de la Clave Privada: Almacenamiento Local
Publicación del Certificado y Clave Pública: Active Directory.

4. Definición de Políticas y Prácticas para los Certificados y Autoridades Certificadoras (AC).

4.1. Definición de Políticas.

4.1.1. Para la AC Raíz de Empresa

Políticas para la autenticación de usuarios ante la AC: Esta AC no emitirá certificados a los usuarios, bajo ninguna circunstancia por lo que no existirá el proceso de autenticación.

Políticas de Asuntos Legales. Si el Certificado Digital o la Llave Privada de la AC raíz se viera comprometida, es obligación del administrador a cargo de esta, renovar de inmediato el certificado y la llave privada así como los de su subordinada y publicar dentro de su CRL el certificado comprometido de manera indefinida.

Políticas del Uso de los Certificados Emitidos por esta AC. Los certificados emitidos por esta AC son de uso EXCLUSIVO para las AC subordinadas.

Políticas para el manejo de Llaves Privadas. La Llave privada de esta AC, debe ser exportada hacia un dispositivo de almacenamiento externo con el fin de protegerla en un lugar seguro.

Políticas para la exportación de Llaves Privadas. La llave privada de esta AC, debe estar disponible para exportarse.

Políticas para el Usuario del Certificado. Por ser los usuarios de estos certificados las AC subordinadas es responsabilidad de los administradores de cada estas proteger la seguridad de las mismas.

Políticas para el Ciclo de Vida de los Certificados. El ciclo de vida de los certificados que emite esta AC debe estar en dependencia de los siguientes factores:

- Longitud de la Llave Privada.
- Seguridad proporcionada por el proveedor de servicios criptográficos.
- Firmeza de la tecnología criptográfica que se utilice.
- La seguridad que se provea a los Certificados y su Llave Privada.

Políticas de Algoritmos Criptográficos a ser usados. Se debe utilizar, algoritmos criptográficos lo suficientemente robustos, para que proporcionen el grado necesario que la implementación de esta AC raíz requiere.

Políticas para la longitud mínima de la Llave Pública y Llave privada. La longitud mínima que deben tener ambas llaves es 2048 bits.

Políticas de emisión y renovación de certificados de esta AC:

- El certificado de esta AC será emitido automáticamente cuando se instale por primera vez en Windows 2000.

' El certificado para las AC Subordinadas será emitido solo cuando éstas últimas lo soliciten.

' El periodo de renovación del certificado de esta AC deben hacerse por lo menos 1 vez en todo su ciclo de vida para asegurar que se le emitan certificados nuevos a las AC subordinadas.

' El período de renovación de los certificados que emiten deberán hacerse como mínimo 1 vez en todo su ciclo de vida. La renovación de certificados se hará en el tiempo establecido en el paso anterior siempre y cuando los certificados y las llaves no se vean comprometidas, queda abierta la posibilidad de renovar mas del tiempo estipulado en aquellos casos que sea necesario.

Políticas para la Publicación de la Lista de Revocación de Certificados (CRL):

' Esta AC debe de constar con su propia CRLs para los certificados que emite.

' Esta AC debe de contar con puntos de Distribución que faciliten la publicación de las CRLs.

' Los puntos de Distribución en los que pueden ser publicadas las CRLs serán: Active Directory, Fólderes Compartidos.

' Los intervalos de Publicación de las CRLs no debe excederse a una Semana, con el objetivo de brindar seguridad e información actualizada.

Políticas para revocar Certificados:

' El certificado de una AC será revocado de manera permanente, cuando este o su clave privada se vea comprometido por falta de seguridad a los mismos.

' El certificado de una AC será revocado cuando esta sea reemplaza o removida permanentemente del servicio para la cual fue designada.

4.1.2. Para la AC Subordinada de Empresa.

Políticas de Asuntos Legales: Si el Certificado Digital o la Llave Privada de la AC subordinada se viera comprometida, es obligación del administrador a cargo de esta, renovar de inmediato el certificado y la llave privada solicitándola de forma manual a la AC raíz, y luego re-emitir los certificados que ya haya emitido. También se debe publicar dentro de la CRL de esta AC el certificado comprometido de manera indefinida.

Políticas del Uso de los Certificados Emitidos por esta AC. Los certificados emitidos por esta AC son de uso EXCLUSIVO para los usuarios o equipos miembros del dominio principal.

Políticas para el manejo de Llaves Privadas. La Llave privada de esta AC, debe ser exportada hacia un dispositivo de almacenamiento externo con el fin de protegerla en un lugar seguro.

Políticas para la exportación de Llaves Privadas. La llave privada de esta AC, debe estar disponible para exportarse.

Políticas para el Usuario del Certificado.Es responsabilidad de cada usuario proteger la seguridad del certificado que le proporcione esta AC.

Políticas para el Ciclo de Vida de los Certificados. *El* ciclo de vida de los certificados que emite esta AC debe estar en dependencia de los siguientes factores:

- Longitud de la Llave Privada.
- Seguridad proporcionada por el proveedor de servicios criptográficos.
- Firmeza de la tecnología criptográfica que se utilice.
- La seguridad que se provea a las AC y su Llave Privada.
- La seguridad que se provea a los Certificados y su Llave Privada.
- Grado de Confianza que se tenga en los usuarios.

Políticas de Algoritmos Criptográficos a ser usados. Se debe utilizar, algoritmos criptográficos lo suficientemente robustos, para que proporcionen el grado necesario que la implementación de esta AC subordinada de empresa requiere.

Políticas para la longitud mínima de la Llave Pública y Llave privada. La longitud mínima que deben tener ambas llaves es 1024 bits.

Políticas de emisión y renovación de certificados de esta AC:

' El certificado de esta AC será emitido por la AC Raíz la primera vez que se instale.

' El periodo de renovación del certificado de esta AC debe hacerse por lo menos 1 vez en todo su ciclo de vida para asegurar que se le emitan certificados nuevos a los usuarios y equipos.

' El período de renovación de los certificados que emiten deberán hacerse como mínimo 1 vez en todo su ciclo de vida.

' La renovación de certificados se hará en el tiempo establecido en el paso anterior siempre y cuando los certificados y las llaves no se vean comprometidas, queda abierta la posibilidad de renovar mas del tiempo estipulado en aquellos casos que sea necesario.

Políticas para la Publicación de la Lista de Revocación de Certificados (CRL):

' Esta AC debe de tener su propia CRLs para los certificados que emite.

' Esta AC debe de contar con puntos de Distribución que faciliten la publicación de las CRLs.

' Los puntos de Distribución en los que pueden ser publicadas las CRLs serán: Active Directory, Fólderes Compartidos.

' Los intervalos de Publicación de las CRLs no debe excederse a una Semana, con el objetivo de brindar seguridad e información actualizada.

Políticas para revocar Certificados:

' El certificado de un usuario será revocado de manera inmediata, cuando éste deje de laborar en la entidad que se lo proporcionó.

' El certificado de un usuario será revocado de manera permanente, cuando éste o su clave privada se vea comprometido por falta de seguridad a los mismos.

' El certificado será revocado de manera permanente, cuando el usuario haga mal uso de los privilegios de confianza que se le otorgan con el certificado.
' El certificado será revocado de manera permanente, cuando el usuario extravíe el certificado por falta de seguridad, quedando expuesto al mal uso de parte de terceros.

' El certificado de una computadora será revocado cuando esta sea reemplaza o removida permanentemente del servicio para la cual fue designada.

' Se revocarán los certificados de las AC que se encuentren dentro de la Jerarquía de Confianza cuando éste o sus Llaves Privadas se vean comprometidos por falta de seguridad.

4.1.3. Para la AC Subordinada Independiente.

Políticas de Asuntos Legales. Si el Certificado Digital o la Llave Privada de la AC subordinada se viera comprometida, es obligación del administrador a cargo de esta, renovar de inmediato el certificado y la llave privada solicitándola de forma manual a la AC raíz, y luego re-emitir los certificados que esta ya haya emitido. También se debe publicar dentro de la CRL de esta AC el certificado comprometido de manera indefinida.

Políticas del Uso de los Certificados Emitidos por esta AC. Los certificados emitidos por esta AC son de uso EXCLUSIVO para los usuarios no miembros del dominio principal.

Políticas para el manejo de Llaves Privadas: La Llave privada de esta AC, debe ser exportada hacia un dispositivo de almacenamiento externo con el fin de protegerla en un lugar seguro.

Políticas para la exportación de Llaves Privadas. La llave privada de esta AC, debe estar disponible para exportarse.

Políticas para el Usuario del Certificado. Es responsabilidad de cada usuario proteger la seguridad del certificado que le proporcione esta AC.

Políticas para el Ciclo de Vida de los Certificados. *El* ciclo de vida de los certificados que emite esta AC debe estar en dependencia de los siguientes factores:

- Longitud de la Llave Privada.
- Seguridad proporcionada por el proveedor de servicios criptográficos.
- Firmeza de la tecnología criptográfica que se utilice.
- La seguridad que se provea a las AC y su Llave Privada.
- La seguridad que se provea a los Certificados y su Llave Privada.
- Grado de Confianza que se tenga en los usuarios.

Políticas de Algoritmos Criptográficos a ser usados. Se debe utilizar, algoritmos criptográficos lo suficientemente robustos, para que proporcionen el grado necesario que la implementación de esta AC subordinada independiente requiere.

Políticas para la longitud mínima de la Llave Pública y Llave privada. La longitud mínima que deben tener ambas llaves es 1024 bits.

Políticas de emisión y renovación de certificados de esta AC.

- El certificado de esta AC será emitido por la AC Raíz la primera vez que se instale.

- El periodo de renovación del certificado de esta AC debe hacerse por lo menos 1 vez en todo su ciclo de vida para asegurar que se le emitan certificados nuevos a los usuarios y equipos.

- El periodo de renovación de los certificados que emiten deberá hacerse como mínimo 1 vez en todo su ciclo de vida.

- La renovación de certificados se hará en el tiempo establecido en el paso anterior siempre y cuando los certificados y las llaves no se vean comprometidas, queda abierta la posibilidad de renovar mas del tiempo estipulado en aquellos casos que sea necesario.

Políticas para revocar Certificados:

- El certificado de un usuario será revocado de manera inmediata, cuando este deje de laborar en la entidad que se lo proporcionó.

- El certificado de un usuario será revocado de manera permanente, cuando este o su clave privada se vea comprometido por falta de seguridad a los mismos.

' El certificado será revocado de manera permanente, cuando el usuario haga mal uso de los privilegios de confianza que se le otorgan con el certificado.

' El certificado será revocado de manera permanente, cuando el usuario extravíe el certificado por falta de seguridad, quedando expuesto al mal uso de parte de terceros.

' El certificado de una computadora será revocado cuando esta sea reemplaza o removida permanentemente del servicio para la cual fue designada.

' Se revocarán los certificados de las AC que se encuentren dentro de la Jerarquía de Confianza cuando este o sus Llaves Privadas se vean comprometidos por falta de seguridad

Políticas para la Publicación de la Lista de Revocación de Certificados (CRL):

' Cada AC debe de tener su propia CRLs para los certificados que emite.

' Cada AC debe de contar con puntos de Distribución que faciliten la publicación de las CRLs.

' Los puntos de Distribución en los que pueden ser publicadas las CRLs serán: Active Directory, Fólderes Compartidos.

' Los intervalos de Publicación de las CRLs no debe excederse a una Semana, con el objetivo de brindar seguridad e información actualizada.

5. Declaración de Prácticas en la gestión de Certificados.

Las prácticas de certificados se refieren a los procedimientos o forma como se realiza la gestión de los certificados en cada AC.

5.1 Para la AC Raíz de Empresa.

- Procedimiento de Inscripción: La inscripción de solicitud de certificados en esta AC por parte de las AC subordinadas se realiza a través del asistente para solicitud de certificados, mediante la herramienta MMC (consola de administración de certificados) disponible en cada equipo local y es realizada por el usuario administrador.

- Procedimiento de Renovación: El proceso de renovación de certificados en esta AC se realiza a través de la herramienta MMC (consola de administración de certificados)

disponible en cada equipo local y es realizada por el usuario administrador. El proceso de renovación se realiza según lo especificado en las correspondientes políticas.

- Procedimiento de Revocación. El proceso de revocación de certificados es realizada por el usuario administrador en base a lo definido en las políticas de revocación, esto se lleva a cabo a través de la herramienta MMC del equipo local.

- Procedimiento de Publicación. El proceso de publicación de los certificados de esta AC se realiza en Active Directory y es realiza automáticamente por cada AC.

5.2. Para la AC subordinada de Empresa.

- Procedimiento de Inscripción: La inscripción de solicitud de certificados en esta AC por parte de los usuarios y equipos miembros se realiza de manera automática través del asistente para solicitud de certificados, mediante la herramienta MMC (consola de administración de certificados) disponible en cada equipo local.

- Procedimiento de Renovación: El proceso de renovación de certificados en esta AC se realiza a través de la herramienta MMC (consola de administración de certificados) disponible en cada equipo local y es realizada por el usuario administrador. El proceso de renovación se realiza según lo especificado en las correspondientes políticas.

- Procedimiento de Revocación. El proceso de revocación de certificados es realizada por el usuario administrador en base a lo definido en las políticas de revocación, esto se lleva a cabo a través de la herramienta MMC del equipo local.

- Procedimiento de Publicación. El proceso de publicación de los certificados de esta AC se realiza en Active Directory automaticamente.

5.3. Para la AC subordinada independiente.

- Procedimiento de Inscripción: La inscripción de solicitud de certificados en esta AC por parte de los usuarios y equipos no miembros se realiza a través de la interfaz Web. Esta tarea es realizada por el usuario administrador quien debe de tener un certificado EFS para inscripción de certificados para usuarios y equipos no miembro. Para que un usuario pueda solicitar un certificado de usuario o equipo debe presentarse ante el administrador con una

carta de aprobación por parte de sus superiores, debe presentar una fotocopia ampliada de su cédula y deberá firmar un compromiso de uso del certificado. Las solicitudes hechas a esta AC por cualquier usuario o equipo estarán pendiente por defecto hasta que se emitan manualmente.

- Procedimiento de Renovación: El proceso de renovación de certificados en esta AC se realiza a través de la herramienta MMC (consola de administración de certificados) disponible en esta AC y es realizada por el usuario administrador de forma manual.

- Procedimiento de Revocación. El proceso de revocación de certificados es realizada por el usuario administrador en base a lo definido en las políticas de revocación, esto se lleva a cabo a través de la herramienta MMC del equipo local.

- Procedimiento de Publicación. El proceso de publicación de los certificados de esta AC se realiza en Active Directory y es realiza automáticamente por cada AC.

6. Definición de Estrategias de Confianza de las AC con los usuarios y equipo.

Como ya se mencionó en la primera parte de este diseño, las diferentes autoridades de certificación que se utilicen en este estudio estarán organizadas jerárquicamente. La utilización de una Jerarquía permite que todos los usuarios y equipos que se encuentren dentro de la jerarquía confíen en una única AC raíz sin importar si existen cambios en las AC subordinadas.

Los certificados que emite cada AC llevan consigo una cadena de confianza, llamada Ruta de Certificación que enlaza cada certificado emitido en una cadena en reversa, es decir desde el certificado hasta la CA raíz.

Los certificados que tienen una ruta de certificación válida hacia un certificado raíz que está en el almacenaje de las AC raíz de confianza del usuario o equipo local se les confía para todos los propósitos listados en el certificado. Si el certificado para la AC raíz para una ruta de certificación no está en el almacenaje de la AC raíz de confianza, la ruta de certificación no es de confianza hasta que se agregada.

Para que el servidor VPN confíe en el cliente VPN es requisito imprescindible que los certificados de ambos posean una ruta de certificación que incluya a la AC raíz. Además en los almacenes locales de certificados de ambos equipos deben de estar presente tanto el certificado de la AC raíz como de las AC subordinadas, de la misma manera funciona con los usuarios VPN internos como externos.

7. Definición de aspectos de Seguridad para las AC.

La seguridad de las AC es una de las partes más importantes a la hora de diseñar una PKI. A continuación se detallarán algunos aspectos de seguridad que se implementarán para proteger a cada una de las AC que forman parte de la PKI.

- Se utilizará Proveedores de Servicios Criptográficos reforzados en la AC raíz y las AC subordinadas, a fin de garantizar la máxima seguridad de estas.

- Se utilizará una Jerarquía de AC con el objetivo que la AC raíz (la más importante) no tenga necesidad de emitir a usuarios disminuyendo considerablemente la carga de la misma y proporcionando una alta disponibilidad de los servicios que prestan.

- Cada una de la AC que se utilicen estará ubicada en un cuarto dedicado al Departamento Informática y serán custodiados por agentes de seguridad a fin de evitar el acceso no autorizado a los mismos.

- Cada AC estará a cargo de un administrador de AC (cuando sea posible) que velará por el buen funcionamiento de las mismas.

- Se utilizará longitudes de llaves Privadas robustas tanto para la AC raíz, como para la AC intermedia.

8. Definición de estrategias de mantenimiento.

Se debe estar claro que una PKI al igual que todas las tecnologías de seguridad, también es vulnerable a fallas de operación provocadas por el mal funcionamiento de los equipos sobre los cuales están instaladas o en el peor de los casos por ataques de terceros

que buscan provocar daños o robar información de las empresas que operan este sistema de seguridad.

Es por eso, que la parte de mantenimiento de una PKI es una etapa trascendental que debe de diseñarse con mucho cuidado y empeño para evitar el menor contratiempo posible.

A continuación se detallarán algunas medidas o prácticas de prevención que se tomarán en la implementación de la PKI.

8.1. Prácticas Preventivas para Servidores

- Se debe de proveer servicios de AC duplicados, de tal manera que si un servidor deja de funcionar en algún momento, otro que esté en línea puede emitir los correspondientes certificados.

- Se respaldaran las AC con bastante frecuencia, de tal manera que puedan ser recuperadas con un mínimo de perdida.

- Se Mantendrán registros de todos los servidores así como de su configuración, para que en caso de algún desastre puedan ser recuperadas con la configuración inicial.

8.2. Prácticas de Seguridad para los Servidores de las AC

- Se mantendrán los servidores de las AC en cuartos seguros, donde estará restringido el acceso físico.

- Se realizarán monitoreos de las auditorias de seguridad en los servidores.

- Se restringirá el acceso al grupo de administradores únicamente a los usuarios encargadas de cada una de las AC.

- Se deshabilitará todos los servicios que no sean necesarios en los servidores de las AC, que puedan facilitar la entrada de intrusos, que puedan afectar el desempeño y la operación de las mismas.

- El desarrollo de una nueva AC se regirá en base a políticas y procedimientos de seguridad.

8.3. Desarrollo de un Plan de Recuperación

El plan de recuperación que se presentará a continuación, tendrá como propósito ayudar a restaurar a las AC si los servidores se ven afectados o si se ve comprometida la AC por falta de seguridad.

- Si los servidores de las AC presentan algún problema físico, como daño de la tarjeta madre, adaptador de red o disco duro, se procederá a reemplazar el dispositivo afectado y restaurar la copia de seguridad más reciente que se tenga. Cuando se trate de la tarjeta madre del servidor, es mejor poner a funcionar el servidor emergente que se tenga disponible ya que el tiempo de reactivación del servidor afectado puede ser un poco larga.

- Si cualquiera de las AC se ve comprometida realizar los siguientes pasos:

  + Revocar el certificado de la AC comprometida de tal manera que se invalide a la AC y sus AC subordinadas, al mismo tiempo que los certificados emitidos por esa AC y sus subordinadas.

  + Publicar una CRL conteniendo el certificado revocado de la AC.

  + Remover los certificados de la AC comprometida del Almacén de Autoridades de Certificación Raíz Confiadas y de las Listas de Confianza de Certificados.

  + Notificar a todos los usuarios afectados y administrador de la AC comprometida e informarle que los certificados emitidos por esa CA serán revocados.

  + Reparar el daño causado desarrollando nuevas AC o renovarles el certificado en caso de ser subordinadas generando además una nueva llave privada. Luego de esto se deben re-emitir los certificados a los usuarios, y computadoras que lo necesiten.

C. Implementación

La tercera y última etapa es la etapa de la implementación. En esta etapa se muestra paso a paso el procedimiento que se debe seguir para instalar y configurar una PKI

que brinde servicios de certificados digitales para los propósitos establecidos en el análisis y diseño. Cabe aclarar que el alcance de esta etapa se limita a la configuración de cada una de las AC y a la emisión de los certificados necesarios para la autenticación de los usuarios y equipos VPN ante el servidor VPN.

1. Ubicación de la PKI en la infraestructura de red Interna.

Tanto la AC raíz de empresa, la AC subordinada de empresa y la AC subordinada independiente se encuentran en las instalaciones de la SEJUVE.

Los equipos que se utilizan para la PKI son los siguientes:

1.1. AC raíz de Empresa.

- Servidor IBM Xseries 205.
- Procesador Intel XEON.
- Memoria Ram 512 MB.
- 2 Disco Duros de 35 GB Ultra-SCI.

1.2. AC subordinada de Empresa.

- Computadora Clon.
- Procesador AMD ATHLON XP 2000 1.6 Mhz.
- Memoria Ram 256 Mb.
- Disco Duro 40 GB IDE.

1.3. AC subordinada de Empresa.

- Computadora Clon.
- Procesador AMD ATHLON XP 2000 1.6 Mhz.
- Memoria Ram 256 Mb.
- Disco Duro 40 GB IDE.

La Siguiente figura ilustra la ubicación física y lógica de las AC dentro de la red interna de la SEJUVE

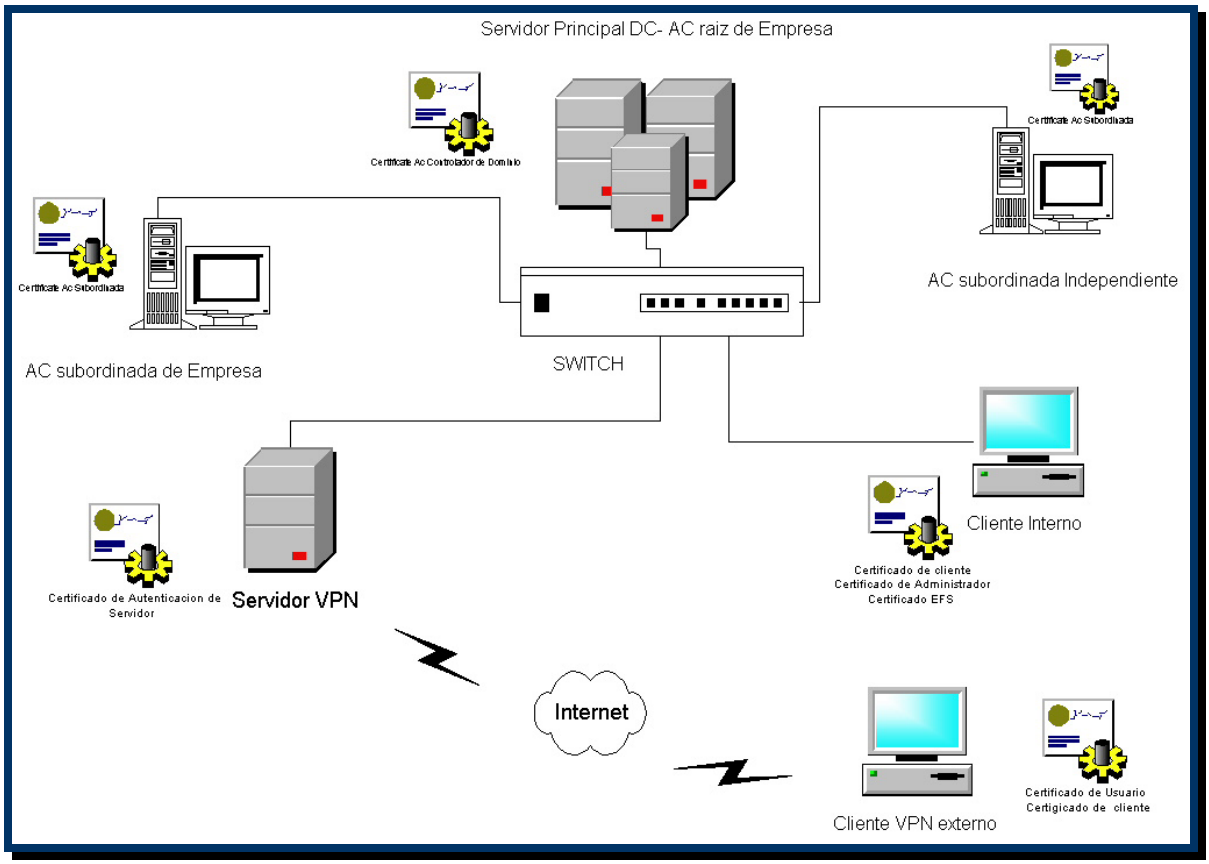


Ilustración IV-2: Ubicación física y lógica de las AC en la RED SEJUVE.

2. Instalación de la AC Raíz de empresa

La instalación y configuración de la AC raíz debe ser la primera cuando se desarrolla una PKI ya que ella es la base de la cadena de confianza de toda PKI.

Antes de describir los pasos a seguir es importante destacar algunos requerimientos básicos que deben de estar presentes antes de iniciar con la instalación de esta AC y que no se explican con detalles porque están fuera del alcance de este estudio.

2.1. Requerimientos previos a la Instalación.

- Debe de estar instalado el sistema operativo Windows 2000 Server (W2K).
- Se debe haber promovido W2K a controlador de dominio principal
- Se deben haber configurado los servicios DNS y DHCP.
- Debe de estar instalado el servicio IIS (Internet Information Server).

Una vez que se han cumplidos estos requerimientos, se procede a instalar la correspondiente AC.

2.2. Instalación de la AC raíz de Empresa.

→ Se introduce el CD de W2K.

→ Se abre el panel de control y se elige Agregar nuevo software -> Agregar componentes de Windows -> Servicios de Certificado.

→ En la pantalla siguiente seleccionar Entidad Emisora raíz de Empresa, opción avanzada y luego siguiente (ilustración IV-3).

→ Las opciones avanzadas me permiten seleccionar entre diferentes tipos de CSP y diferentes longitudes de clave y algoritmos HASH, como se puede constatar en la ilustración IV-4.

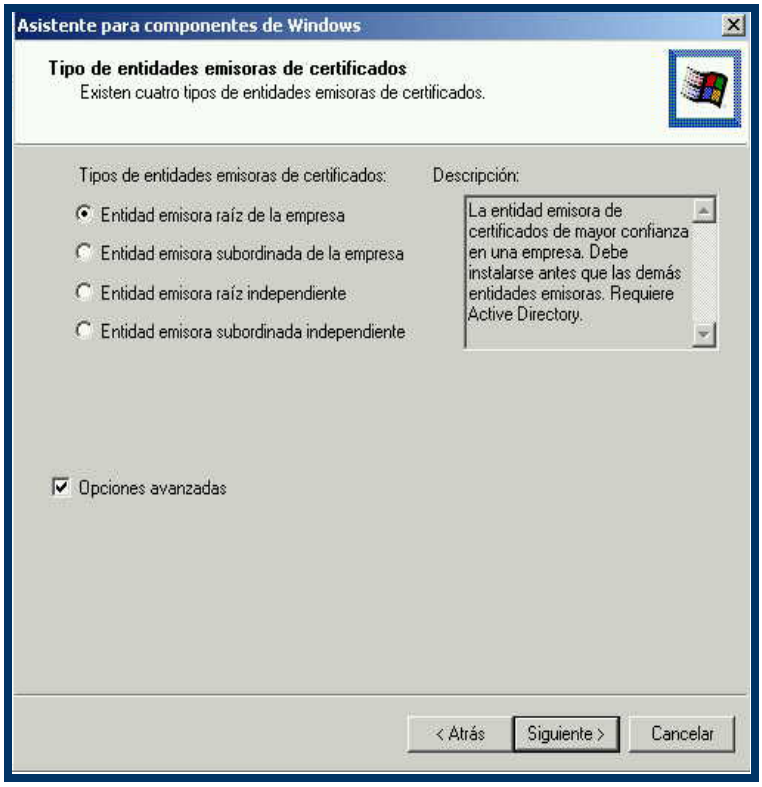


Ilustración IV-3: Ventana de selección de "Tipo de entidades emisoras de certificados".

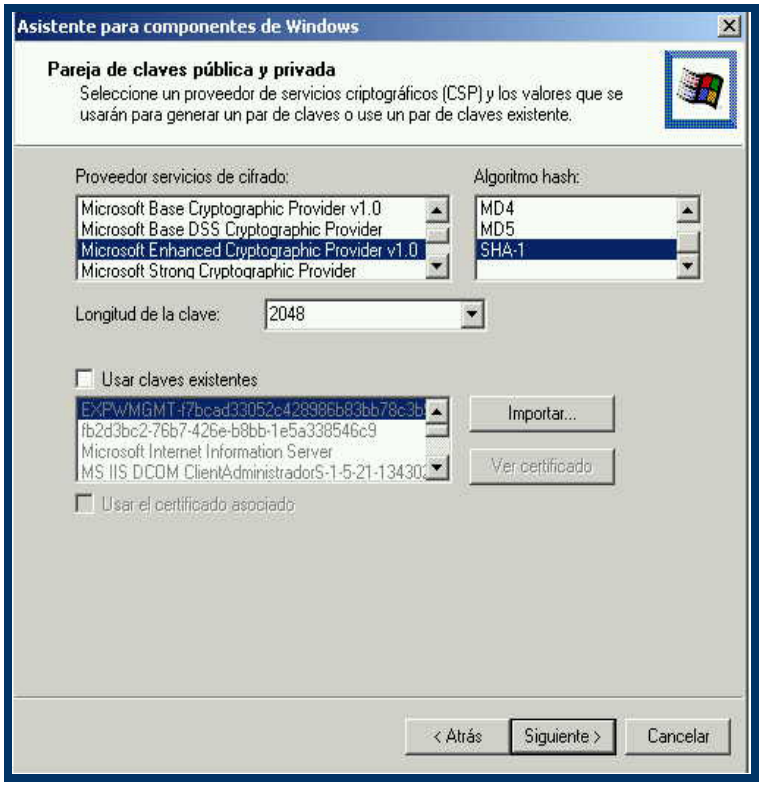


Ilustración IV-4: Ventana de selección de "Pareja de claves públicas y privadas".

→ Se rellena el formulario con los datos básicos de la Entidad Emisora como lo muestra la ilustración IV-5.

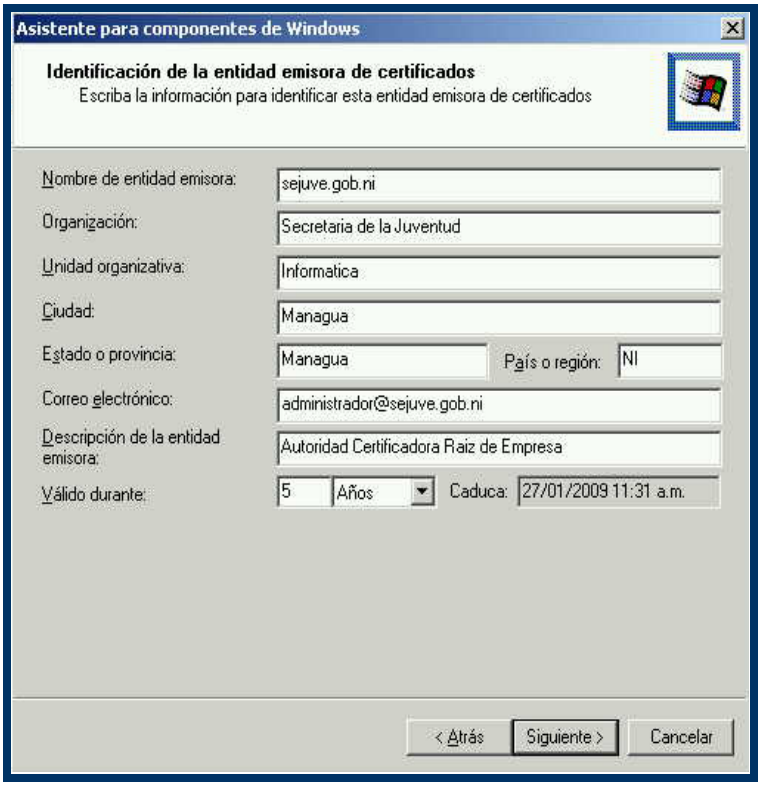


Ilustración IV-5: Ventana de selección para la "Identificación de la entidad emisora de certificados".

→ Se especifica donde se guardará la configuración de los certificados.

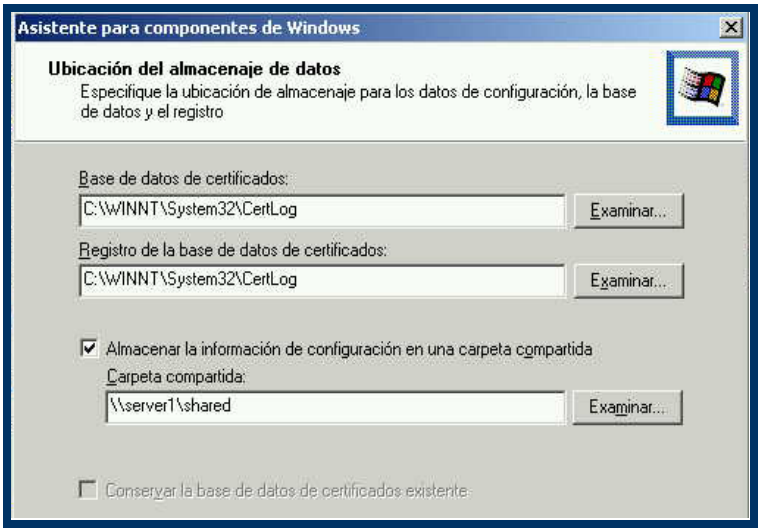


Ilustración IV-6: Ventana de selección de "Ubicación del almacenaje de datos".

→ Con esta información la AC emite y firma un certificado para si misma.

3. Instalación de la AC subordinada de empresa

3.1. Requerimientos previos a la Instalación.

- Debe de estar instalado el sistema operativo Windows 2000 Server (W2K).
- Debe de estar instalado el servicio IIS (Internet Information Server).
- El servidor debe ser miembro del servidor principal.

3.2. Instalación de la AC subordinada de Empresa.

→ Se introduce el CD de W2K.

→ Se abre el panel de control y se elige Agregar nuevo software -> Agregar componentes de Windows -> Servicios de Certificado.

→ Seleccionar Entidad Emisora subordinada de Empresa, opción avanzada y luego siguiente. (ilustración IV-7 y IV-8).

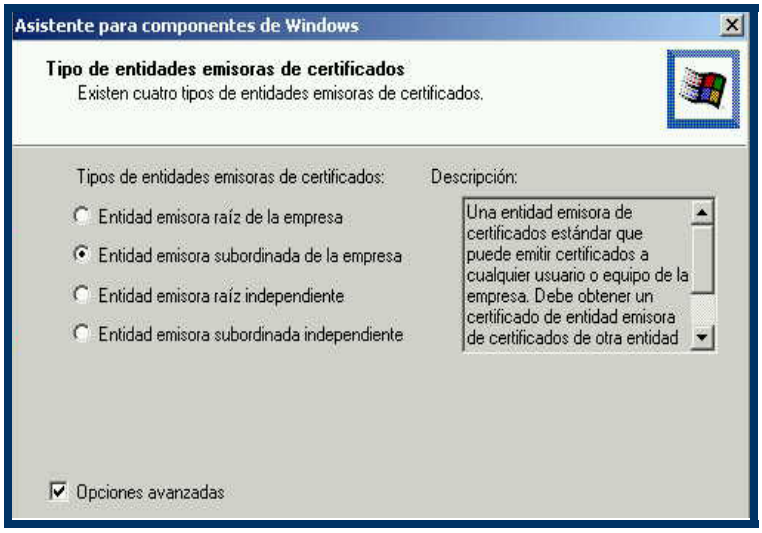


Ilustración IV-7: Instalación de la AC. Ventana de selección de "Tipo de entidad emisoras de certificados".

→ Seleccionar lo que indica la pantalla.

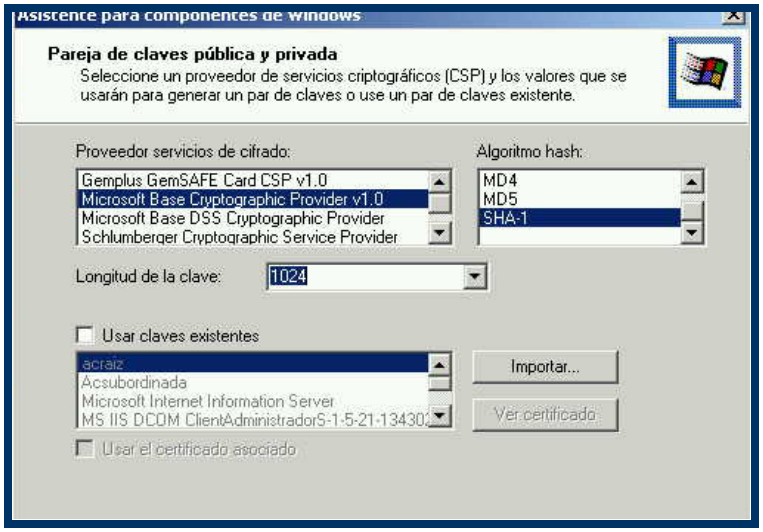


Ilustración IV-8: Instalación de la AC. Ventana de selección de "Pareja de claves públicas y privada".

→ Se rellena el formulario con los datos básicos de la entidad emisora.

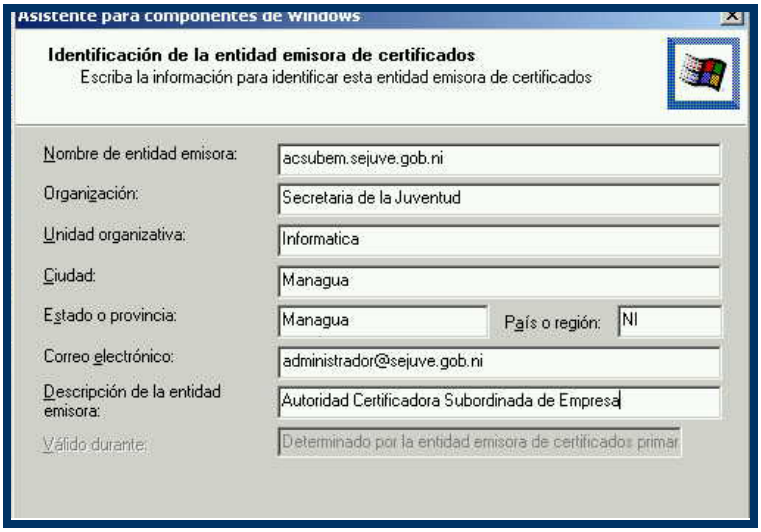


Ilustración IV-9: Instalación de la AC. Ventana de selección de "Identificación de la entidad emisora de certificados".

→ Se especifica donde se almacenará la configuración de los certificados, al igual que se hizo con la AC raíz empresa.

→ A diferencia de la AC raíz de empresa que firma y emite su propio certificado, la AC subordinada de empresa realiza la solicitud del mismo a la AC raíz la jerarquía, como lo muestra la ilustración IV-10.

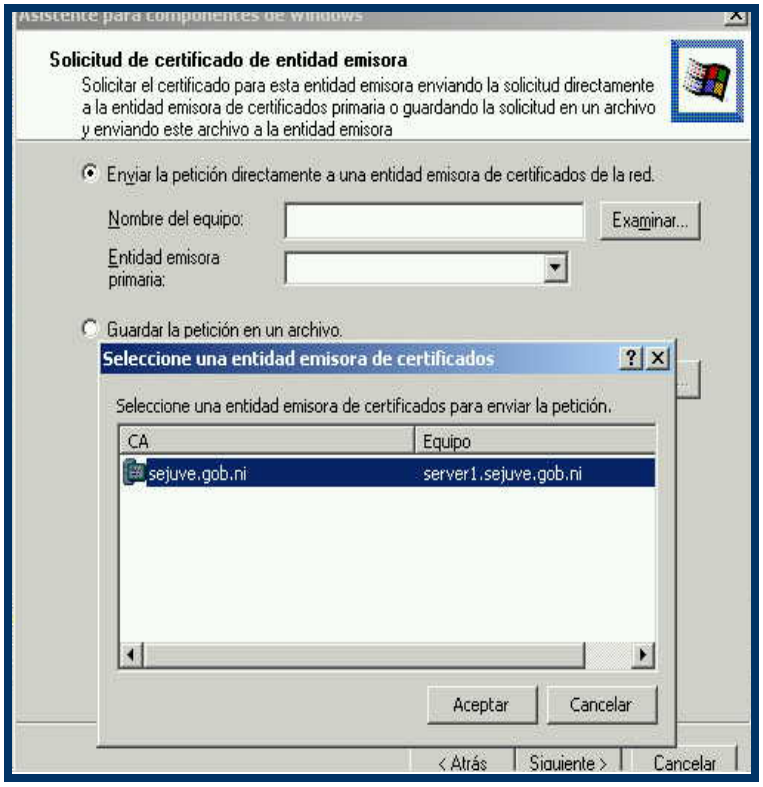


Ilustración IV-10: Instalación de la AC. Ventana de la selección de "Solicitud de certificado de entidad emisora".

→ Una vez realizado estos pasos la AC subordinada empresa, obtiene un certificado de la raíz y se coloca en el segundo nivel en la jerarquía.

4. Instalación de la AC subordinada independiente.

4.1. Requerimientos previos a la Instalación.

- Debe de estar instalado el sistema operativo Windows 2000 Server (W2K).
- Debe de estar instalado el servicio IIS (Internet Information Server).
- El servidor debe ser miembro del servidor principal.

4.2. Instalación de la AC subordinada de Empresa.

→ Se introduce el CD de W2K.

→ Se abre el panel de control y se elige Agregar nuevo software -> Agregar componentes de Windows -> Servicios de Certificado.

→ El procedimiento que se sigue para la instalación de esta AC es similar al de la anterior, lo único que cambia es el tipo de AC, que en este caso es subordinada independiente y la información de identificación de la AC.

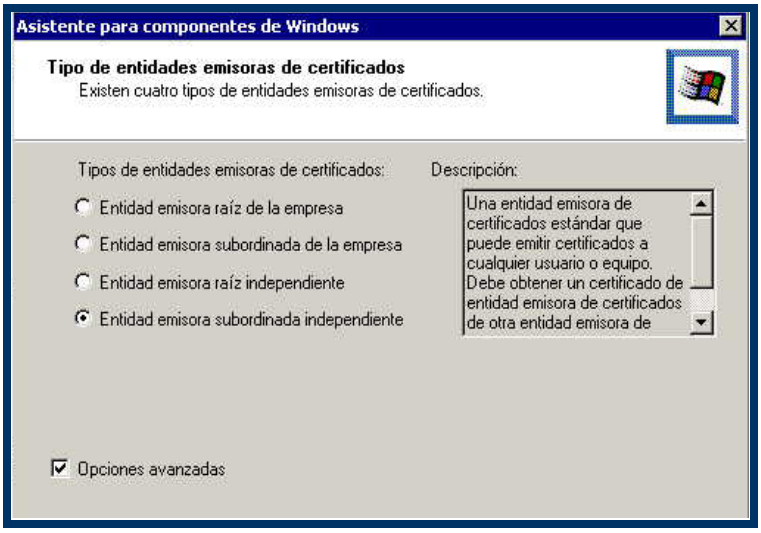


Ilustración IV-11: Instalación de la AC subordinada "Tipo de entidades emisoras de certificados".

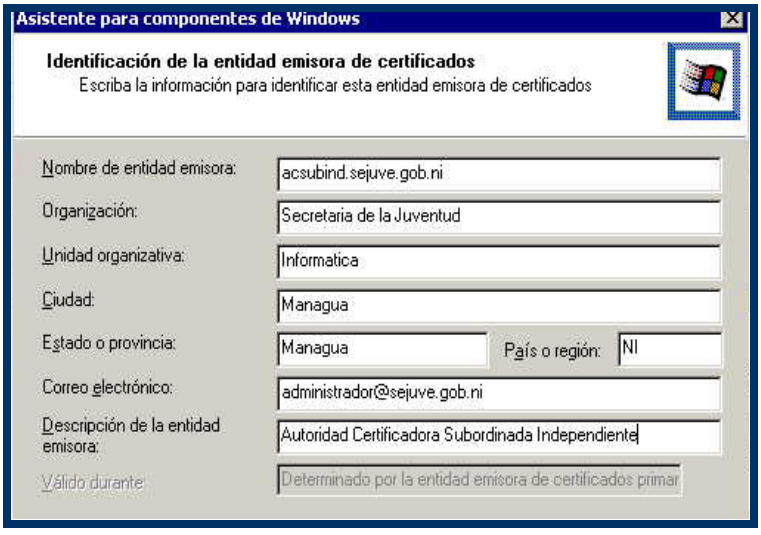


Ilustración IV-12: Instalación de la AC Subordinada "Identificación de la entidad emisora de certificados".

5. Verificación de las rutas de certificación.

Una vez instalada la Jerarquía de Certificación como se había previsto, es necesario corroborar que las rutas de certificación de cada una de ellas están configuradas adecuadamente, para eso abrimos la consola de administración de certificados de cada una de los equipos y verificamos las rutas de certificación como lo muestra las ilustraciones.

5.1. Autoridad Certificadora Raíz de Empresa.

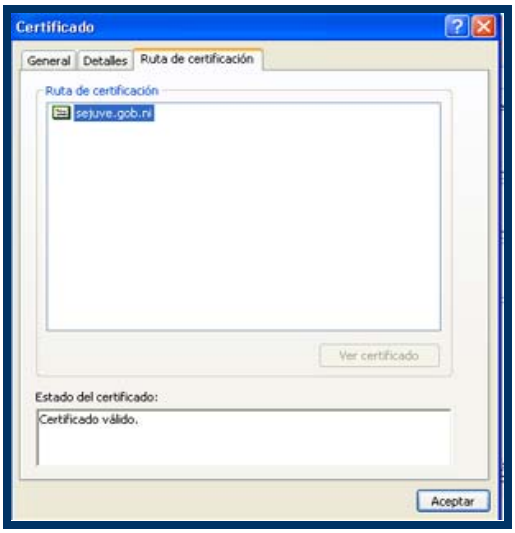


Ilustración IV-13: Ruta de Certificación de la Autoridad Certificadora Raíz de Empresa.

5.2. Autoridad Certificadora Subordinada Independiente.

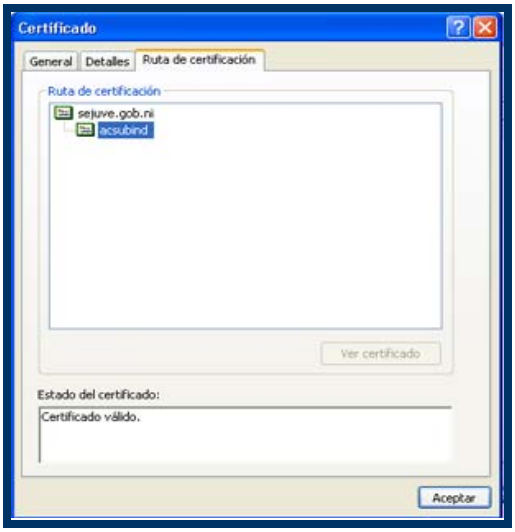


Ilustración IV-14: Ruta de Certificación de la Autoridad Certificadora Subordinada Independiente.

5.3. Autoridad Certificadora Subordinada de Empresa.

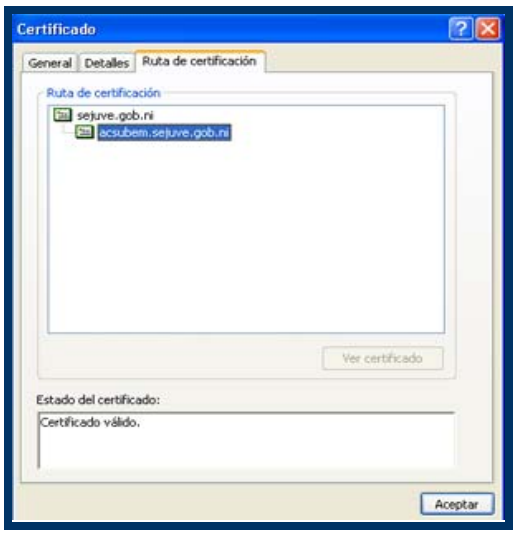


Ilustración IV-15: Ruta de Certificación de la Autoridad Certificadora Subordinada de Empresa.

Una vez verificado que las rutas de certificación estén configuradas adecuadamente se proceden a emitir los certificados necesarios para la VPN con el protocolo L2TP. Las solicitudes de los certificados para estos fines se realizan de la siguiente manera:

- Usuarios y equipos miembros del dominio: La emisión de los certificados lo realiza la AC subordinada de Empresa.

- Usuarios y equipos no miembros del dominio: La emisión de los certificados lo realiza la AC subordinada Independiente.

6. Solicitud y emisión de certificados a utilizar

En éste estudio se necesitan certificados para usuarios y equipos que forman parte y que no forman parte del dominio de la SEJUVE. La AC encargada de emitir certificados a los miembros será la AC subordinada de Empresa y emitirá certificados de administrador para el encargado de manejar la PKI y un certificado EFS para permitirle a esa persona encargada poder solicitar certificados para equipos y usuarios no miembros.

A continuación se detallan los procedimientos que se deben seguir para poder obtener estos tipos de certificados.

6.1. Administrador y EFS.

Los certificados de administrador y EFS serán emitidos a aquella persona que se encargue tanto de la administración de la PKI como de solicitar los certificados para equipos y usuarios no miembros del dominio principal.

- La solicitud de certificados se hace desde el contenedor de certificados del usuario actual.
- Las plantillas de certificados que se utilizan son plantilla administrador y plantilla EFS básico.

La ilustración IV-16 muestra la ventana donde se seleccionan los tipos de certificados disponibles, según las directivas de la AC subordinada de empresa.

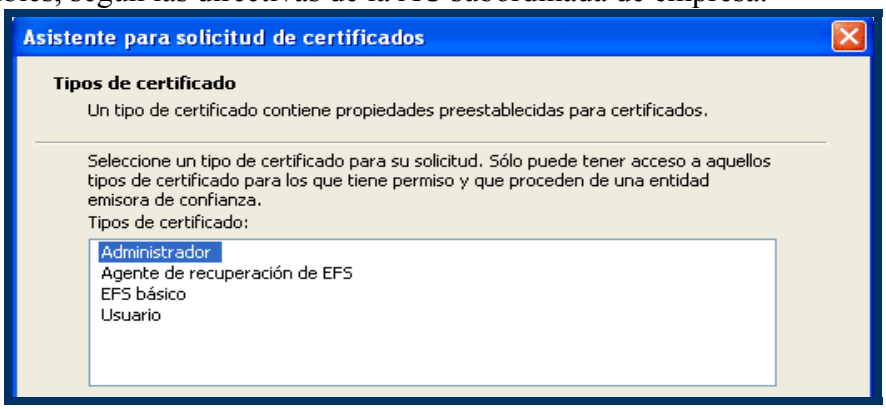


Ilustración IV-16: Ventana de selección de "Tipos de certificados".

Para el certificado de administrador se utiliza el CSP Microsoft Enhanced Cryptographic Provider v 1.0 con clave de 1024 bits.

Ilustración IV-17: Ventana de selección de "Asistente para solicitud de certificados".

Para el certificado de EFS se utiliza el CSP Microsoft Enhanced Cryptographic Provider v 1.0 con clave de 512 bits.

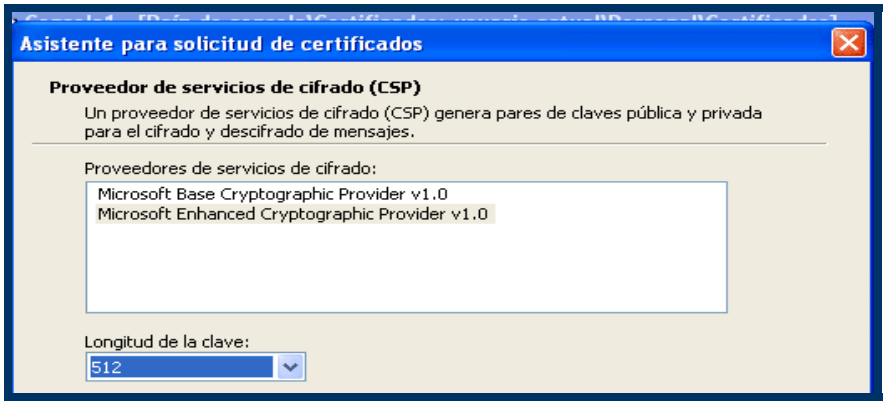


Ilustración IV-18: Certificación del EFS.

La ventaja de solicitar certificados siendo miembros del dominio de la SEJUVE, es que la relación de confianza con las AC Raíz y AC intermedia se realizan de manera automática.

Una vez que se le han emitidos los certificados de administrador y EFS a la persona encargada de la PKI, esta debe de solicitar los certificados tanto para el servidor VPN, como para los clientes a los que se les autorice el acceso.

6.2. *Servidor VPN (no miembro del dominio).*

Los certificados de los equipos y usuarios no miembros son emitidos por la AC subordinada independiente y solicitados por el administrador. Las solicitudes de este tipo se realizan a través de la interfaz Web de la AC correspondiente.

El único inconveniente con este tipo de solicitudes, es que al no ser los usuarios y equipos miembros del dominio principal la relación de confianza debe de realizarse de forma manual. Esto significa que se debe incluir en el contenedor de AC raíz y AC intermedias los respectivos certificados.

→ Entrar a la interfaz Web de la AC subordinada independiente. http://acsubind/certsrv. (Ilustración IV-19)

Ilustración IV-19: Interfaz Web de la AC Subordinada.

→ Elegir Solicitud Avanzada.

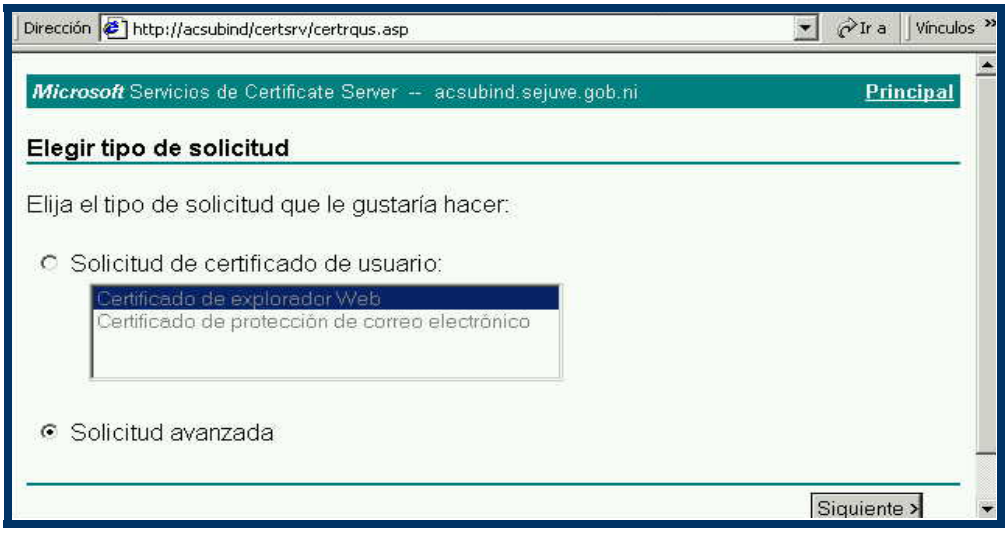


Ilustración IV-20: Ventana de selección de la "Solicitud Avanzada".

→ Seleccionar Enviar una solicitud de Certificado usando una forma.

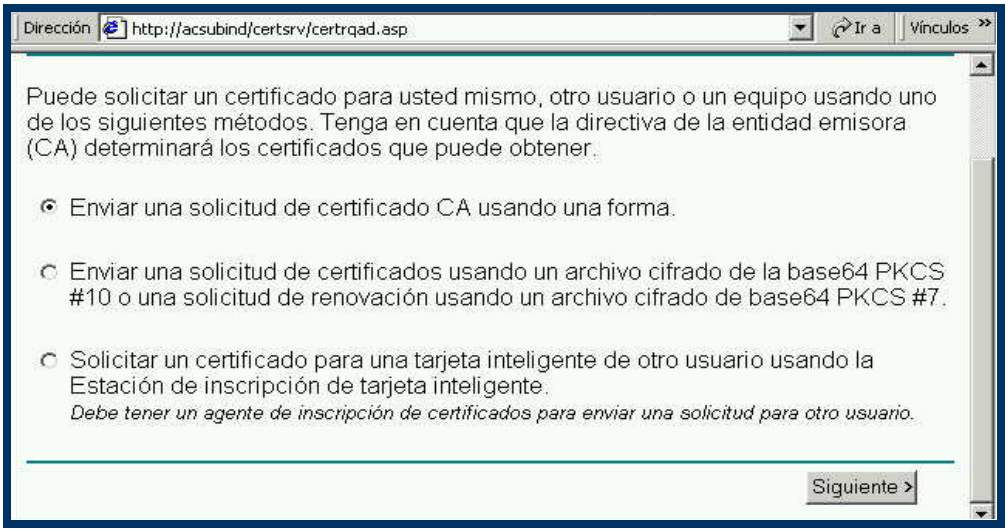


Ilustración IV-21: Envío de la solicitud de Certificado.

→ Introducir datos sobre el equipo VPN

Ilustración IV-22: Solicitud de Certificado Avanzada. Introducción de datos del equipo VPN.

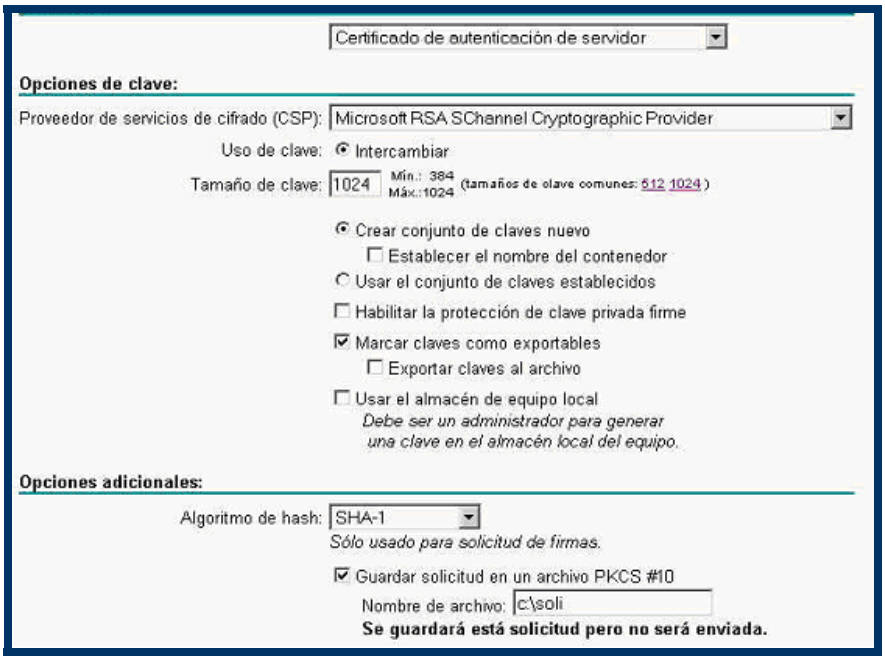


Ilustración IV-23: Datos del equipo VPN.

→ Es importante destacar que la solicitud que se está procesando, debe ser almacenada en un archivo local, lo cual garantiza que una vez que la AC la apruebe se pueda guardar tanto el certificado como la ruta de certificación.

→ Entrar a la interfaz Web de la AC nuevamente, pero esta vez para colocar la solicitud guardada en el archivo local. Para esto se selecciona

"Enviar una solicitud de certificados utilizando archivo cifrado de la Base 64 PKCS # 10".

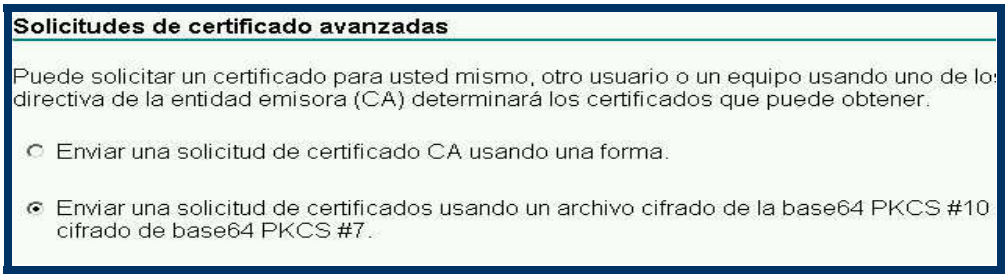


Ilustración IV-24: Interfaz Web de la AC. Colocación de la solicitud en el archivo local.

→ Abrir el archivo de la solicitud almacenada localmente y pegarla en el cuadro de texto solicitud de certificado.

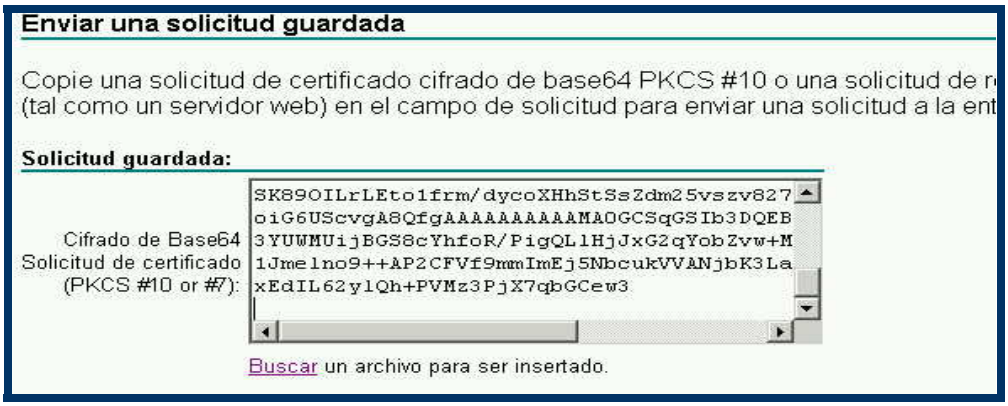


Ilustración IV-25: Envío de una solicitud guardada.

→ Este tipo de solicitudes quedan pendiente por defecto, hasta que el encargado de la AC emita el certificado manualmente.

→ El siguiente paso es confirmar que el certificado haya sido emitido. Esto se realiza mediante la interfaz Web.

→ El último paso consiste en descargar el certificado y la ruta de certificación emitidos para que sean instalados en los correspondientes equipos.

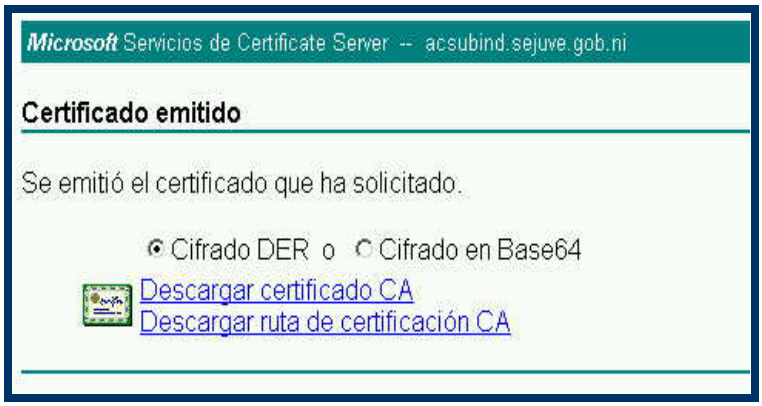


Ilustración IV-26: Descargue y emisión del certificado.

7. Certificados para usuario y equipos externos (no miembros del dominio).

Para que a los usuarios externos se les pueda otorgar un certificado para conectarse al servidor VPN, deben presentar los requerimientos que se especifican en las prácticas de gestión para ésta AC. Por defecto ésta AC está configurada para que deje pendiente todas las solicitudes que se le hagan hasta que un administrador los autorice y emita manualmente.

→ El usuario debe presentarse ante el administrador con los documentos que se requieren.

→ E administrador procede a recopilar la información básica del usuario.

→ El administrador teclea la siguiente dirección: http://acsubind/certsrv para entrar a la interfaz Web de la AC subordinada independiente. (ilustración IV-27).

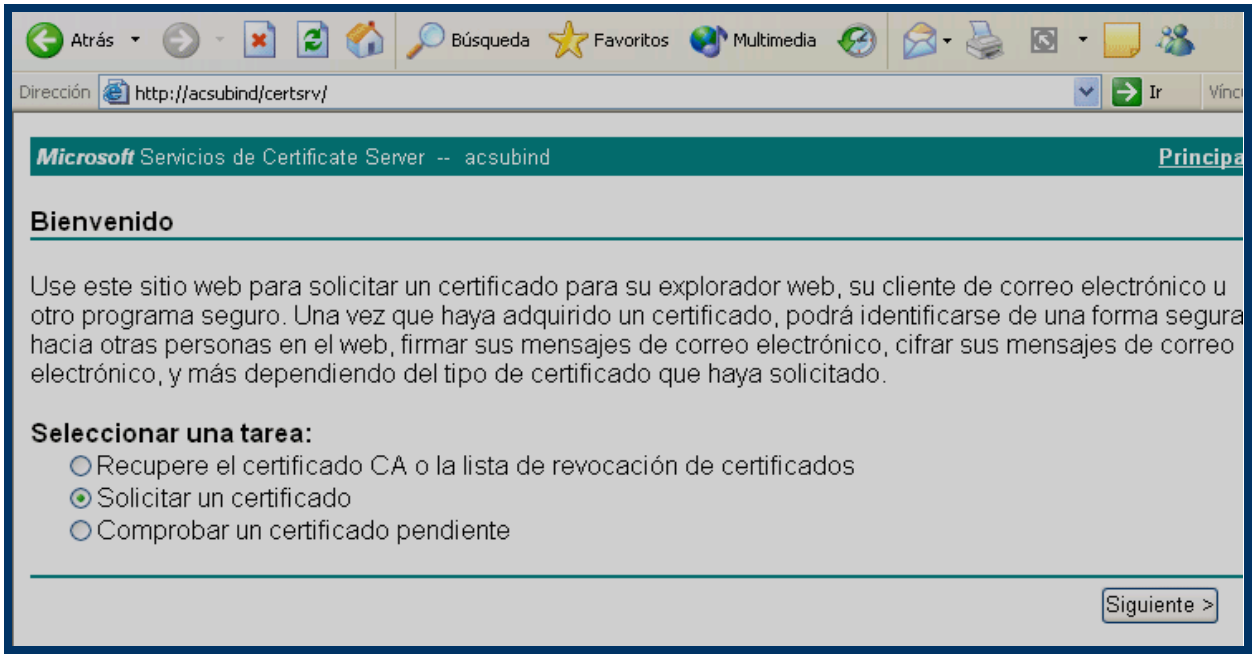


Ilustración IV-27: Interfaz Web AC subordinada Independiente.

→ Elige Solicitud Avanzada en Tipo de Solicitud.

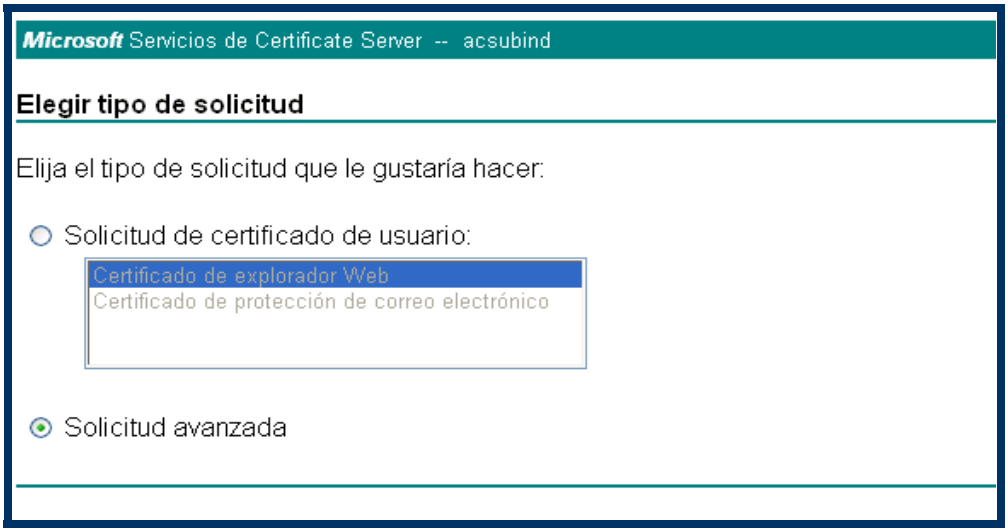
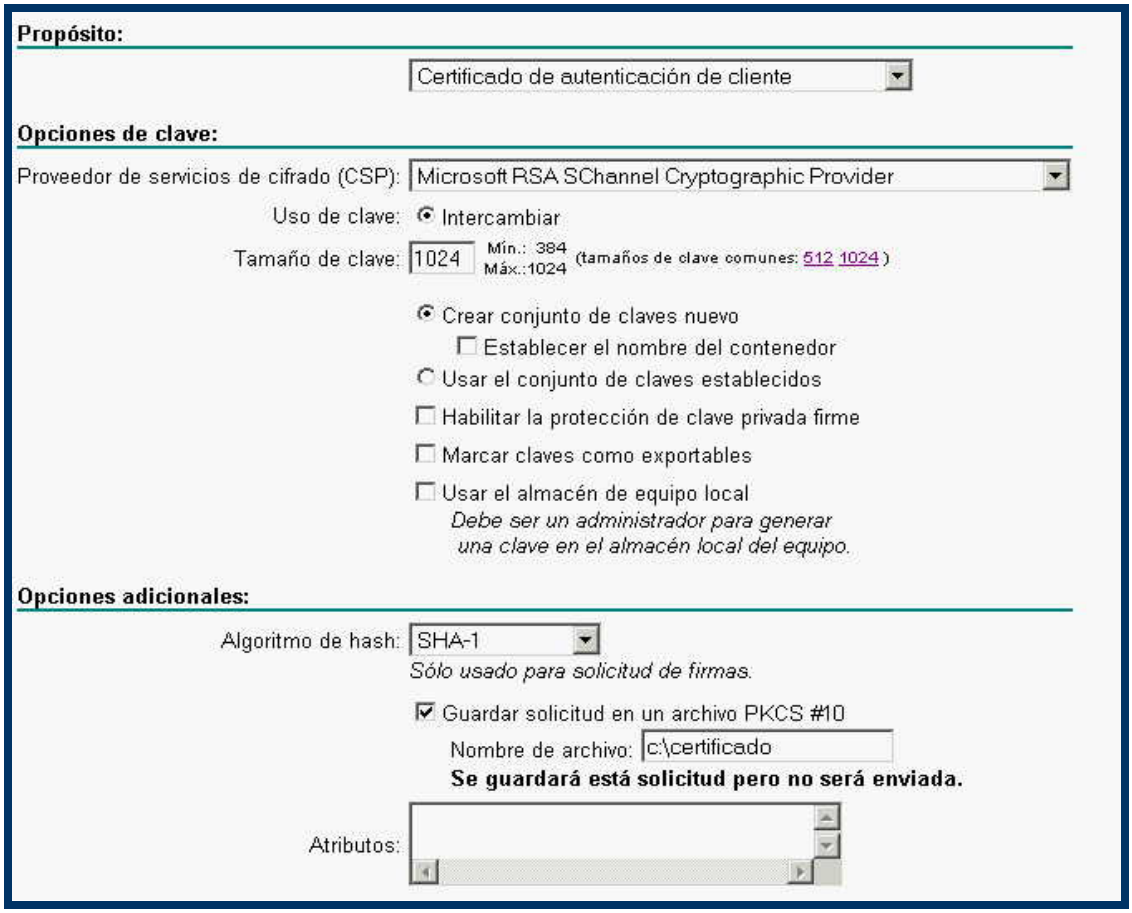


Ilustración IV-28: Tipo de solicitud "Elección de Solicitud Avanzada".

→ Se seleccionar Enviar una solicitud de Certificado CA usando una forma.

→ Se introduce la información básica del usuario al que se le está emitiendo el certificado, así como el tipo de CSP a utilizar y el propósito del certificado, en este caso autenticación de cliente.

Ilustración IV-29: Datos de información de la solicitud de certificado avanzada.



→ El siguiente paso es volver a entrar a la interfaz Web de la AC independiente para enviar la solicitud usando el archivo cifrado PKCS # 10 que se genero en el paso anterior.

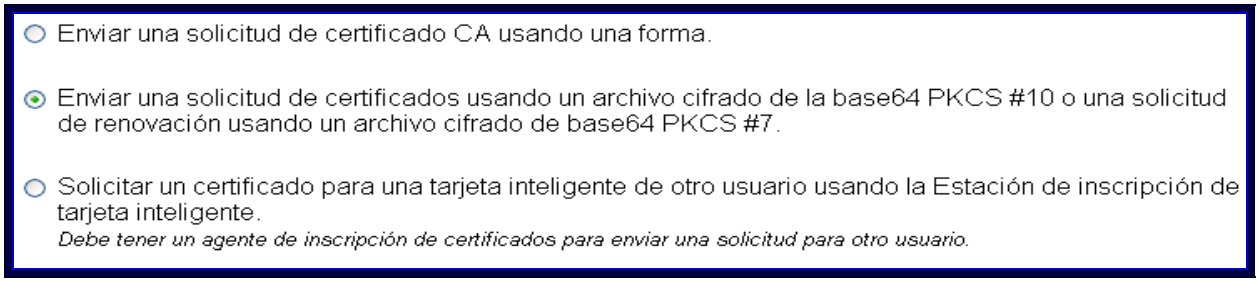
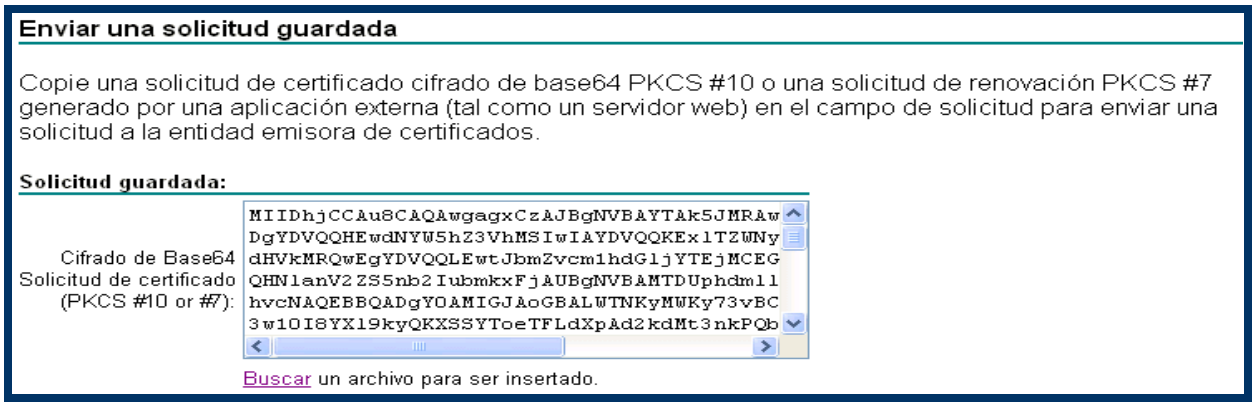


Ilustración IV-30: Envío de solicitud de certificado AC.

→ Se procede a abrir el archivo codificado en un editor de texto como notepad, se selecciona y se copia en el campo del certificado



→ Como se había mencionado, una vez emitida la solicitud a la AC, esta queda pendiente hasta que sea emitida manualmente por el administrador.

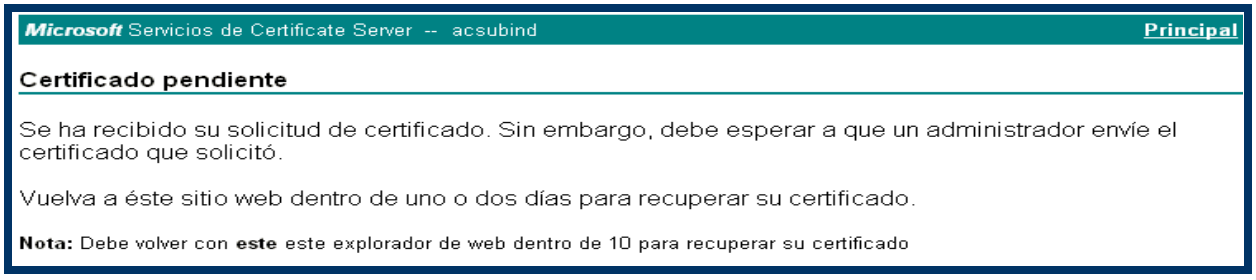


Ilustración IV-31: Certificado pendiente de solicitud a la AC.

→ El administrador debe de entrar a la consola de administración de la AC independiente y emitir el certificado pendiente.

→ Luego, el administrador debe volver a entrar a la interfaz Web para comprobar que el certificado ya esté disponible y descargar tanto el certificado, como su ruta de certificación, como lo muestra la ilustración IV-32.

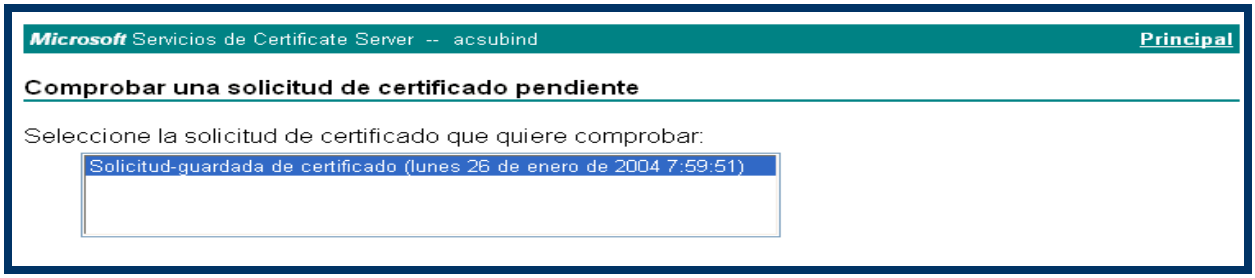


Ilustración IV-32: Comprobación de una solicitud de certificado pendiente.

La ilustración IV-33 muestra la pantalla que se presenta una vez que el certificado solicitado ha sido emitido, quedando pendiente de esa manera únicamente a almacenar el certificado.

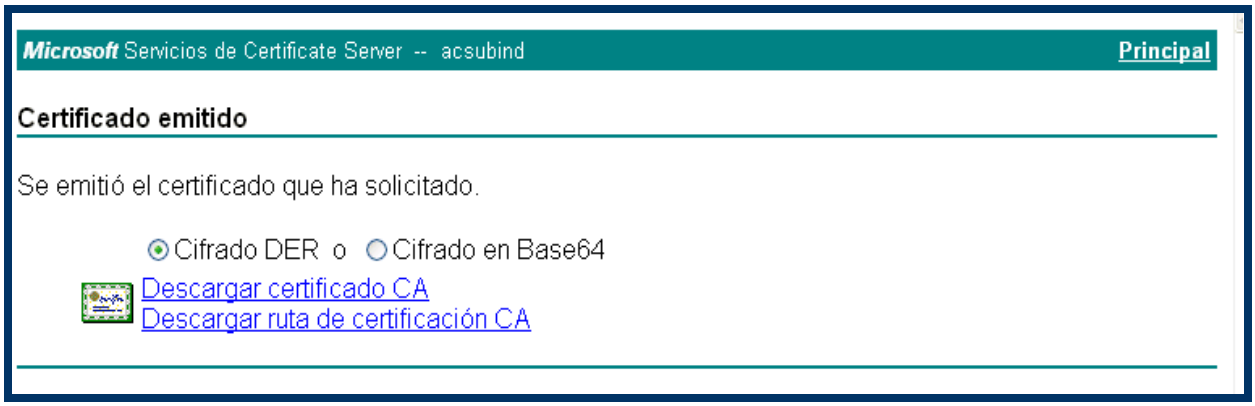


Ilustración IV-33: Certificado Emitido.

Este procedimiento se realiza tanto para los usuarios como para los equipos externos, teniendo el cuidado de seleccionar autenticación de cliente como propósito del certificado.

8. Instalación de los certificados solicitados.

Los certificados que son emitidos por AC tanto raíz como subordinadas de empresa para usuarios y equipos miembros del dominio son instalados automáticamente en los almacenes locales de certificados de dichos usuarios o equipos junto con su correspondiente ruta de certificación.

Para los equipos o usuarios que no son miembros del dominio es necesario que se instalen manualmente los certificados que se les emita certificado. Además de los certificados de los clientes VPN, es necesario instalar el certificado de la AC raíz de la jerarquía con la que se trabaja, en el almacén de certificados de las Entidades Emisoras Raíz de Confianza, de igual forma se debe instalar el certificado de la AC subordinada que emitió el certificado, creándose de esa manera una ruta de certificación o de confianza y permitiendo así que los certificados sean validos para su propósito.

8.1. Instalar Certificado para el servidor VPN.

Una vez que sea ha descargado el certificado para el servidor VPN, y su respectiva ruta de certificación, se procede a instalarlo.

Para realizar este procedimiento es necesario que se entre a la consola de administración de certificados en la cuenta de equipos y seleccionar "Importar certificados en la carpeta personal" como se muestra en la ilustración IV-34.

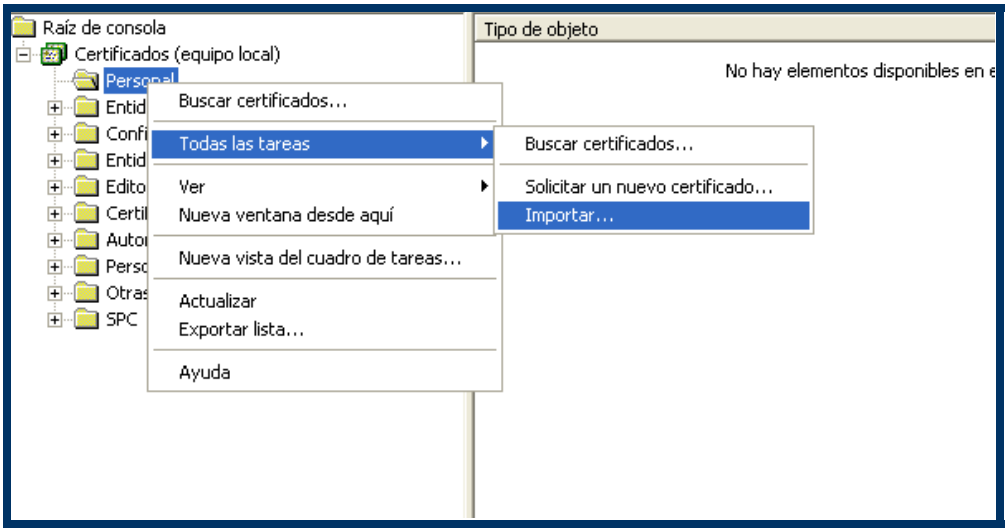


Ilustración IV-34: Consola de administración de certificados.

Se abre el asistente para importar certificados donde luego se tiene que especificar el lugar donde se tiene almacenado el certificado (ilustración IV-35 y IV-36).

Ilustración IV-35: Ventana de "Asistente para importación de certificados".

Ilustración IV-36: Ventana de "Especificación de Archivo para importar".

Es importante especificar el lugar hacia donde se va a importar, como este certificado es de máquina se debe de seleccionar Almacén de certificados “Personal” de la cuenta local, de similar forma a como se muestra en la ilustración IV-37.

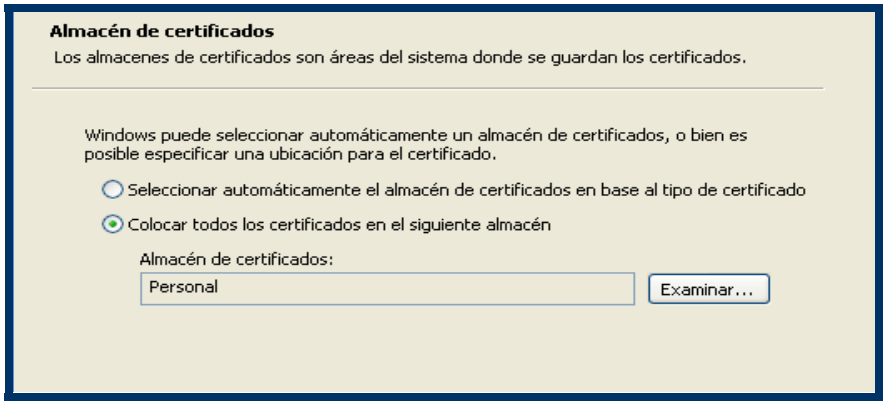
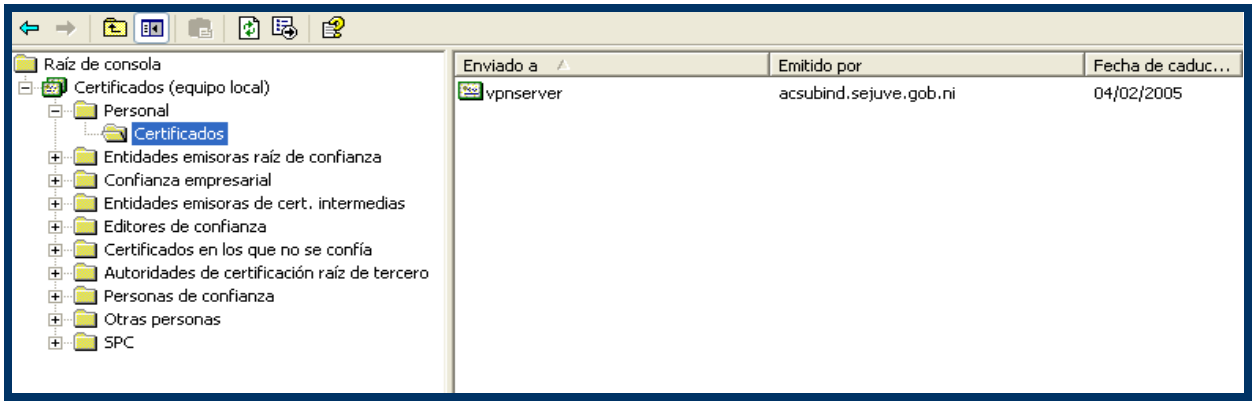


Ilustración IV-37: Ventana de selección del lugar donde se importa el certificado".

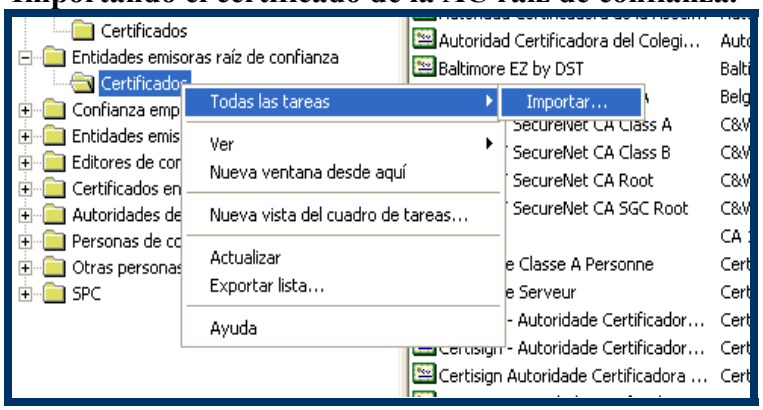
De esa manera el certificado queda instalado en su correspondiente almacén, como se logra apreciar en la siguiente ilustración.



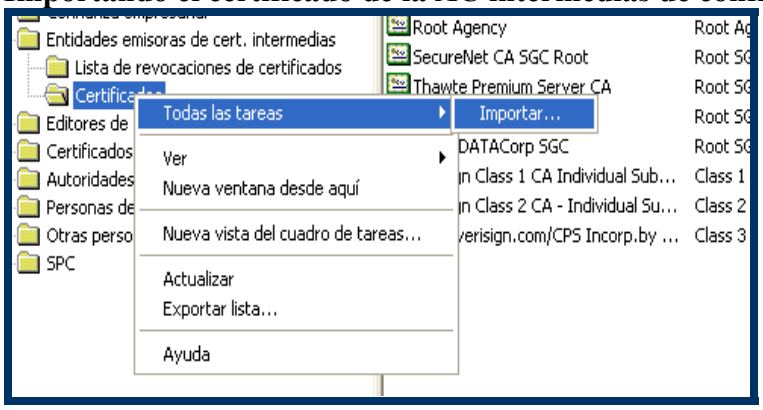
La ruta de certificación que se almacenó junto al certificado posee también tanto el certificado de la AC que emitió el certificado, como el certificado de la AC raíz, de esa manera estos certificados son fácilmente exportables para su correspondiente instalación en los almacenes correspondientes para que se cree una relación de confianza adecuada.

Para instalar los certificados de las dos AC se deben de entrar a la consola de administración de certificados de la cuenta de equipo o usuario local y presionar importar certificado de las entidades emisoras raíz de confianza y de las entidades emisoras de certificados intermedios siguiendo el mismo procedimiento del certificado VPN Server.

Importando el certificado de la AC raíz de confianza.



Importando el certificado de la AC intermedias de confianza.



Este procedimiento permite que tanto el certificado de la AC raíz como de la AC subordinada independiente se instalen para formar parte de la relación de confianza.

Una vez que se instalan los certificado de las AC Raíz e Intermedias correspondiente se puede apreciar que dichos certificados aparecen reflejados en el almacén de certificados, (Ilustración IV-38 y IV-39).

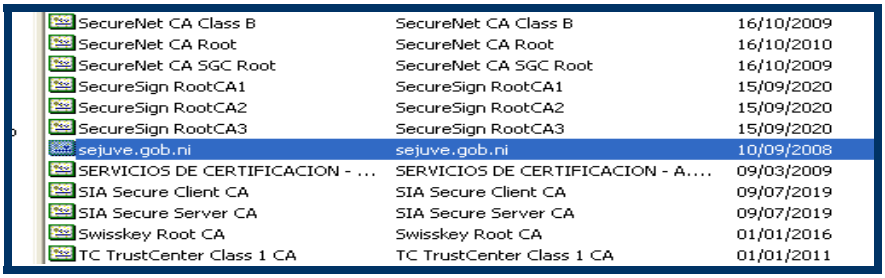


Ilustración IV-38: Certificado de la AC Raíz Instalado.

Ilustración IV-39: Certificado de la AC Subordinada Independiente Instalada.

La ilustración IV-40 muestra la Ruta de Certificación que se crea para el Servidor VPN.

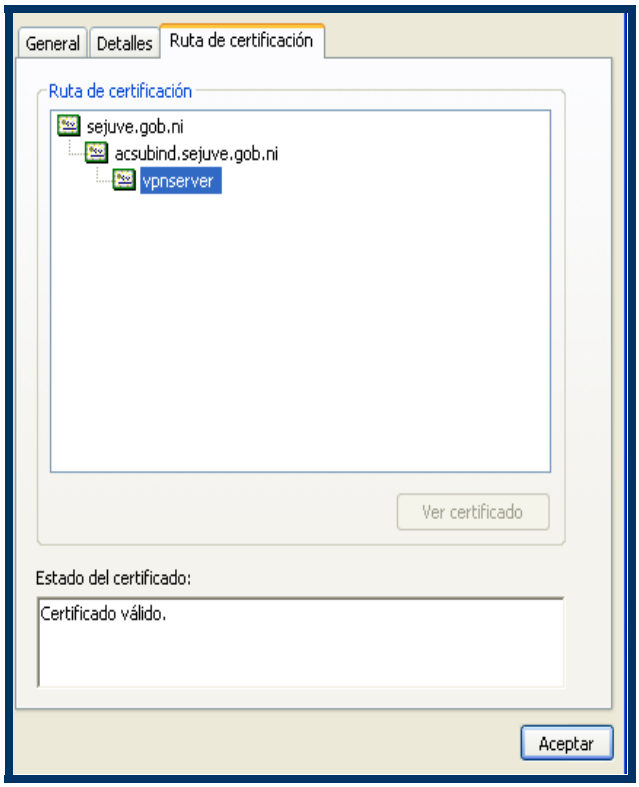
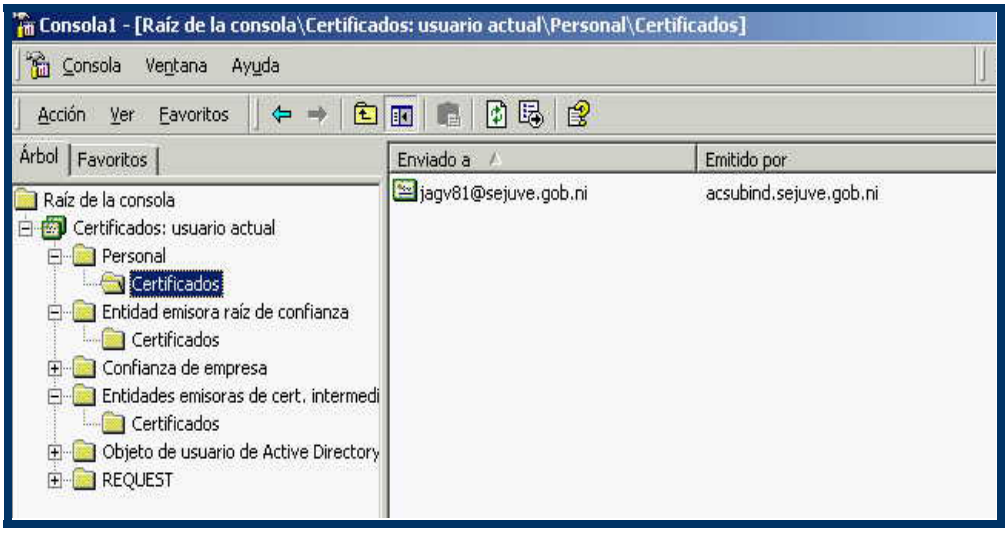


Ilustración IV-40: Ruta de Certificación para el Servidor VPN.

9. Certificado para Usuarios y Cliente VPN.

El procedimiento que se sigue para instalar los clientes VPN es igual al que se mostró para el servidor VPN, con la única diferencia que los certificados se deben importar desde la cuenta de usuario local en la consola de administración de certificados.

Se debe de verificar que los certificados de la AC raíz y de la AC subordinada también se importen adecuadamente para que se establezca la adecuada relación de confianza.



La ilustración IV-41 muestra los Certificado de la AC raíz que se encuentran Instalados.

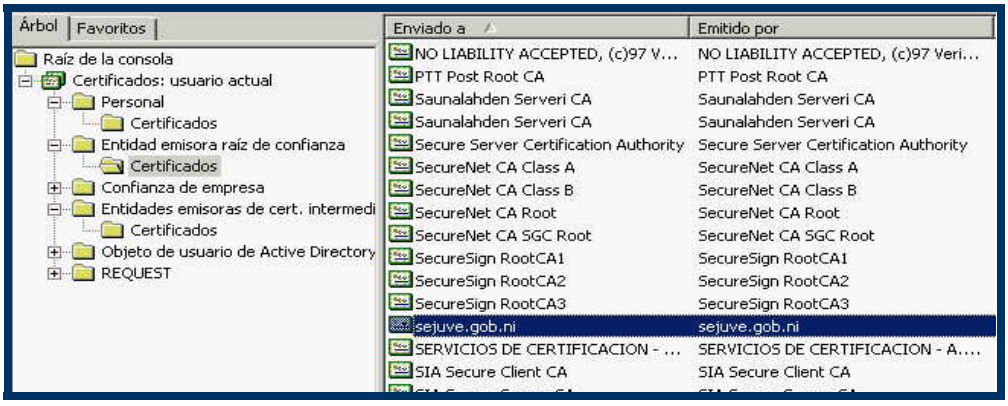


Ilustración IV-41: Certificado de la AC Raíz Instalado.

La ilustración IV-42 muestra los Certificado de la AC intermedias que se encuentran Instalados.

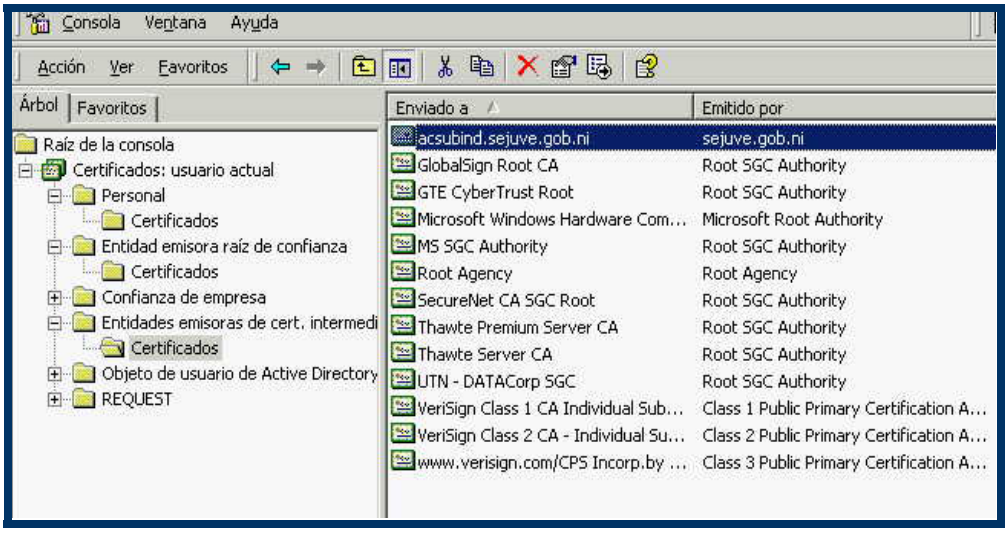


Ilustración IV-42: Certificado de la AC Raíz Instalado.

V. Implementación de una VPN

V. IMPLEMENTACION DE UNA VPN

A. Implementación

Una vez que se han instalado los certificados en los correspondientes equipos, se procede a configurar tanto el servidor como los clientes VPN de acuerdo a lo especificado en el diseño. Esta fase es conocida como fase de implementación y representa la última etapa en el proceso de montaje de una VPN utilizando certificados digitales. Si bien es cierto esta etapa es la más sencilla dentro del proceso se debe de realizar con mucho cuidado a fin de que el resultado sea satisfactorio.

La implementación de la VPN se hará en este estudio detallando paso a paso el procedimiento a seguir para la configuración de todos los equipos involucrados.

1. Instalación de Servidor Principal.

Se debe asegurar que el servidor principal o controlador de dominio, que a su vez funciona como AC raíz de Empresa tenga instalado y configurado las siguientes aplicaciones para el buen funcionamiento de la VPN:

a) El servidor W2K debe de estar configurado como Controlador de Dominio, como lo muestra la ilustración V-1.

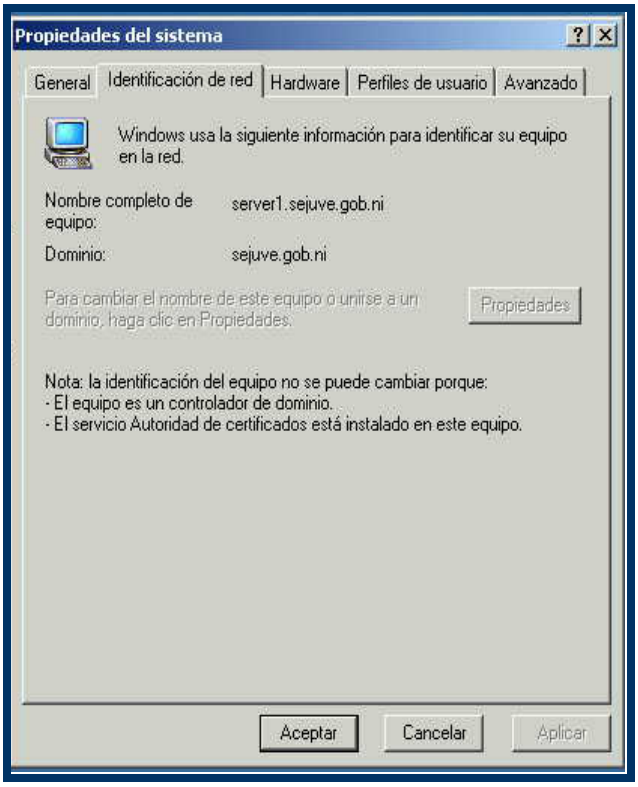


Ilustración V-1: Ventanilla de "Propiedades del Sistema".

b) El servidor W2K debe de permitir la administración de Usuarios a través de Active Directory como lo muestra la ilustración V-2.

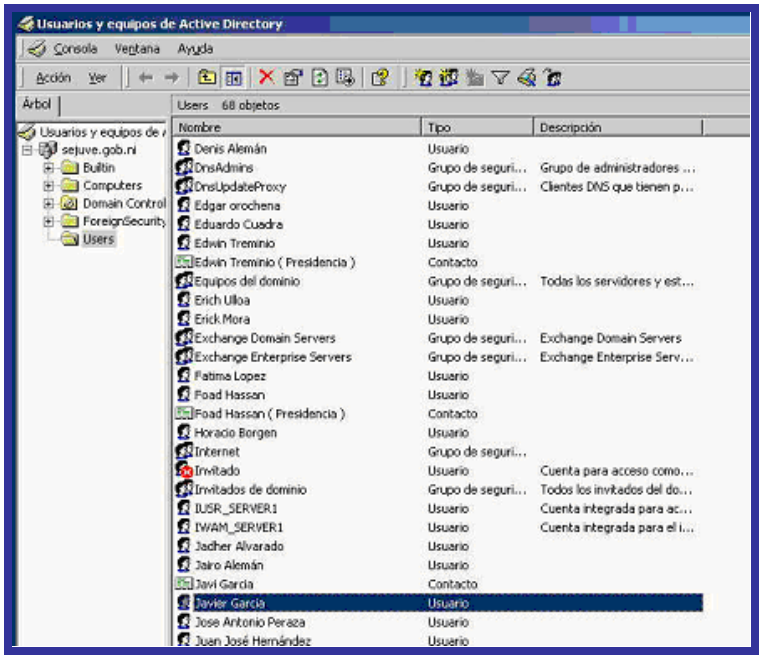


Ilustración V-2: Usuarios y equipos de Active Directory.

c) El Servidor W2K debe de estar configurados para prestar los servicios DHCP y DNS para brindárselos a sus clientes como lo muestra las ilustraciones V-3 y V-4.

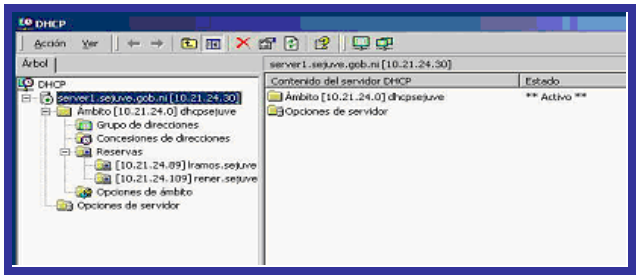


Ilustración V-3: Servidor Principal ofreciendo servicio DHCP

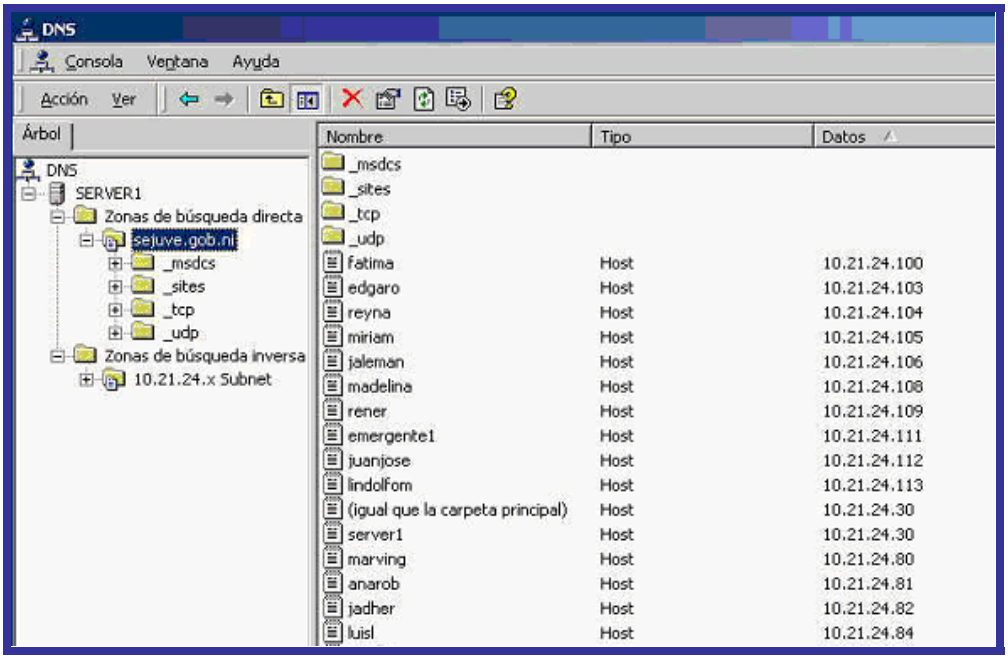


Ilustración V-4: Servidor Principal ofreciendo servicio DNS

d) La interfaz del Servidor W2K debe de estar configurado a como se especificó en la fase de diseño para este equipo. La ilustración V-5 muestra la configuración de la interfaz de red del servidor principal.

.

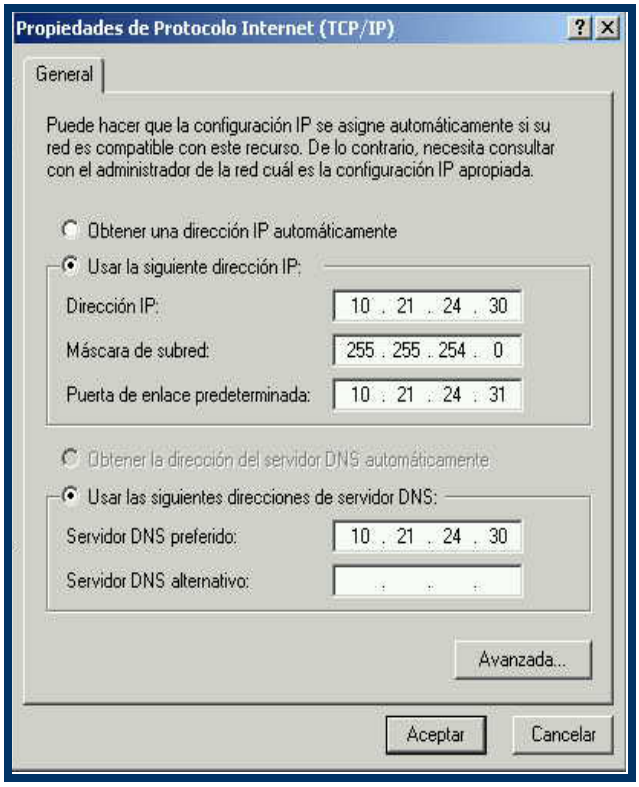


Ilustración V-5: Propiedades de Protocolo Internet (TCP/IP).

Con estas configuraciones básicas, este servidor se convierte en el servidor principal de la institución ya que es el encargado de manejar y administrar los nombres y direcciones de todos los clientes que forman parte de la red SEJUVE.

2. Instalación del Servidor VPN

El proceso de instalación de un Servidor VPN es bastante sencillo, siempre y cuando se especifican claramente todos los parámetros de configuración.

a) La primera fase al igual que el Servidor Principal consiste en instalar el Sistema Operativo completo asegurándose de que sean reconocidos todos los periféricos del equipo, principalmente las 2 interfaces o tarjetas de red que se encuentren presentes en el equipo y que se le asigne el nombre **VPN** al equipo.

b) El servidor VPN posee dos interfaces o tarjetas de red, una de las cuales debe estar configurada con la dirección IP pública que asignó el proveedor y la otra debe estar configurada con una dirección IP privada que permita enrutar los datos o información que llegue a el, hacia una de las interfaces del enrutador principal.

La ilustración V-6 muestra la configuración de la interfaz para manejar el enlace a Internet.

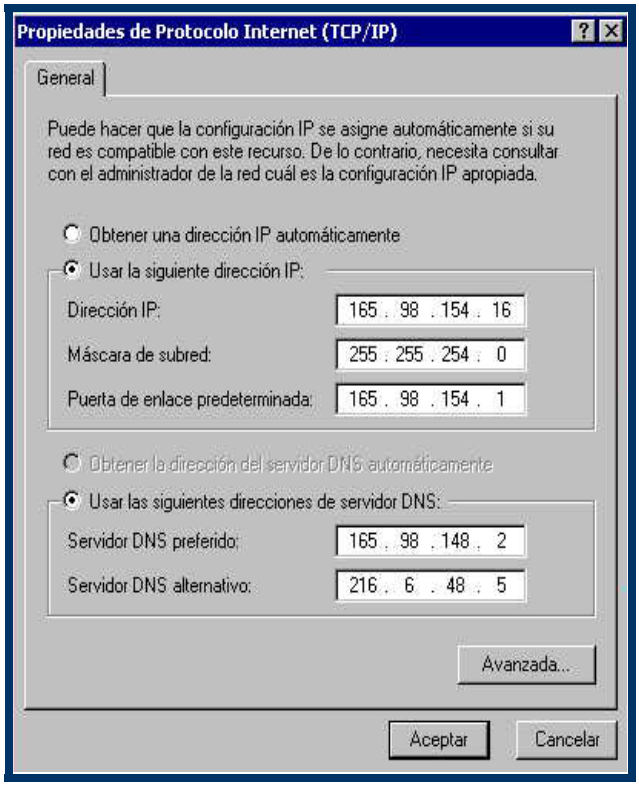
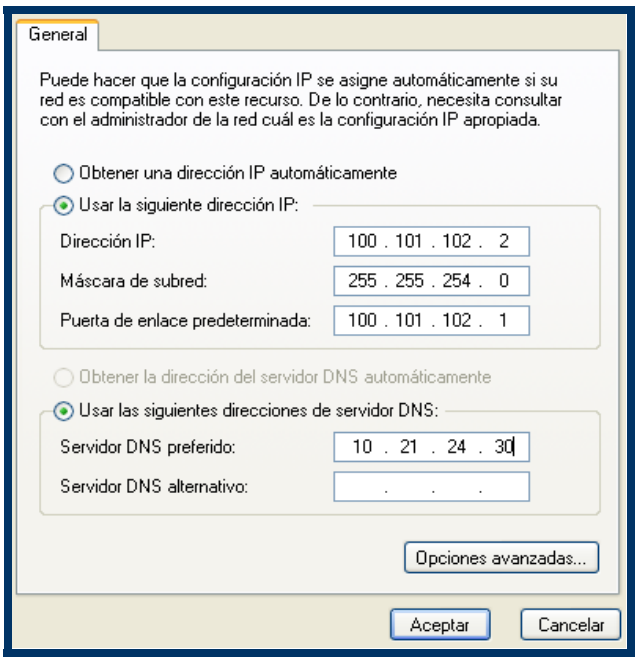


Ilustración V-6: Configuración de la primera Interfaz.

Las direcciones que se observan en la pantalla anterior corresponden a las direcciones asignadas por el proveedor de servicios de Internet que se contrató para estos fines.

b) La otra interfaz, es la que estará conectada a una de las interfaces del enrutador principal. Esta interfase se configura manualmente con la dirección **100.101.102.2** y se conecta a la interfaz del enrutador principal utilizando el cable correspondiente.

La siguiente ilustración muestra la configuración de la interfaz para manejar el enlace a la red Interna.



c) Una vez que el servidor VPN tiene configurado sus dos interfaces principales se procede a configurar la parte medular para la utilización de la VPN. Para configurar la VPN se hace uso de la Herramienta administrativa **Enrutamiento y Acceso Remoto.** El procedimiento que se sigue se detalla a continuación.

→ Iniciar la Herramienta administrativa Enrutamiento y acceso remoto, como lo muestra la ilustración V-7.

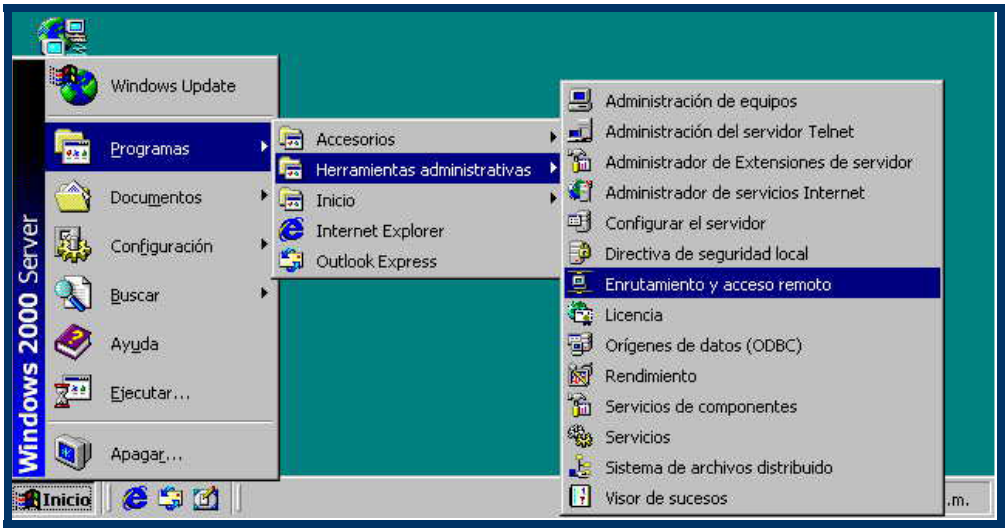


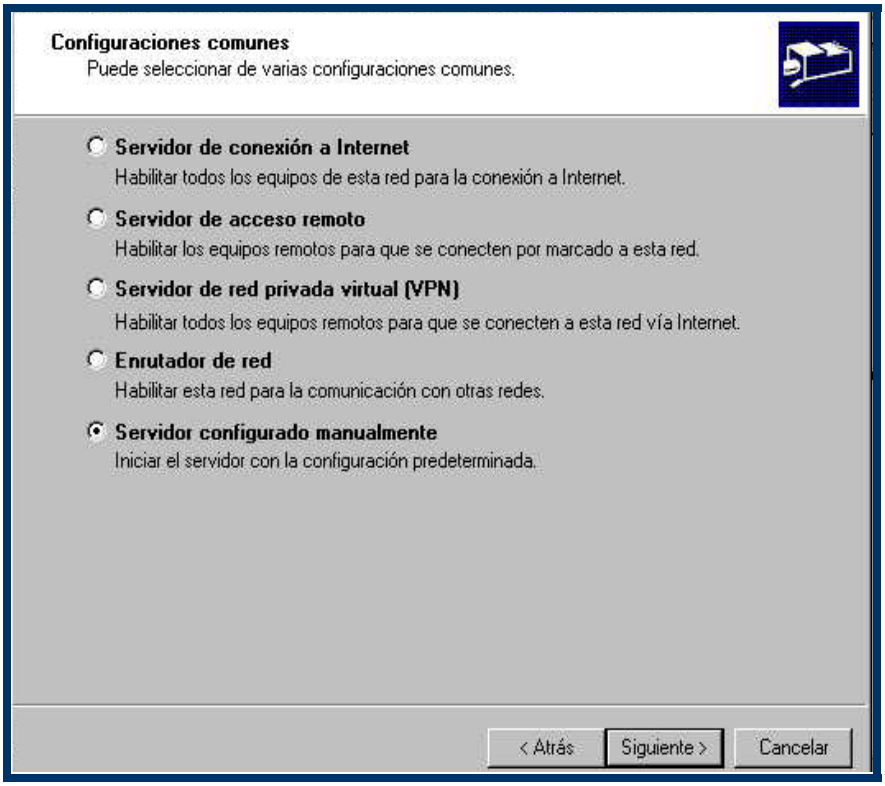
Ilustración V-7: Herramienta Administrativa de Enrutamiento.

Esta herramienta no sólo es utilizada para configurar un servidor VPN, también se utiliza par proveer enrutamiento de datos en las redes de computadora.

→ Se presiona Configurar y habilitar el enrutamiento y el acceso remoto para habilitar el servidor, como se muestra en la ilustración V-8.

Ilustración V-8: Enrutamiento y Acceso Remoto.

→ Se debe de seleccionar la configuración manual entre las opciones disponibles como se muestra en la siguiente ilustración.



→ Existen otras configuraciones comunes para el uso de este servidor, incluso como se puede apreciar existe la opción especifica para una VPN, pero no se debe seleccionar ya W2K no configura adecuadamente el servidor VPN mediante esta opción.

→ Una vez finalizada la selección de servidor configurado manualmente se procede a iniciarlo, como se muestra en la figura V-9.

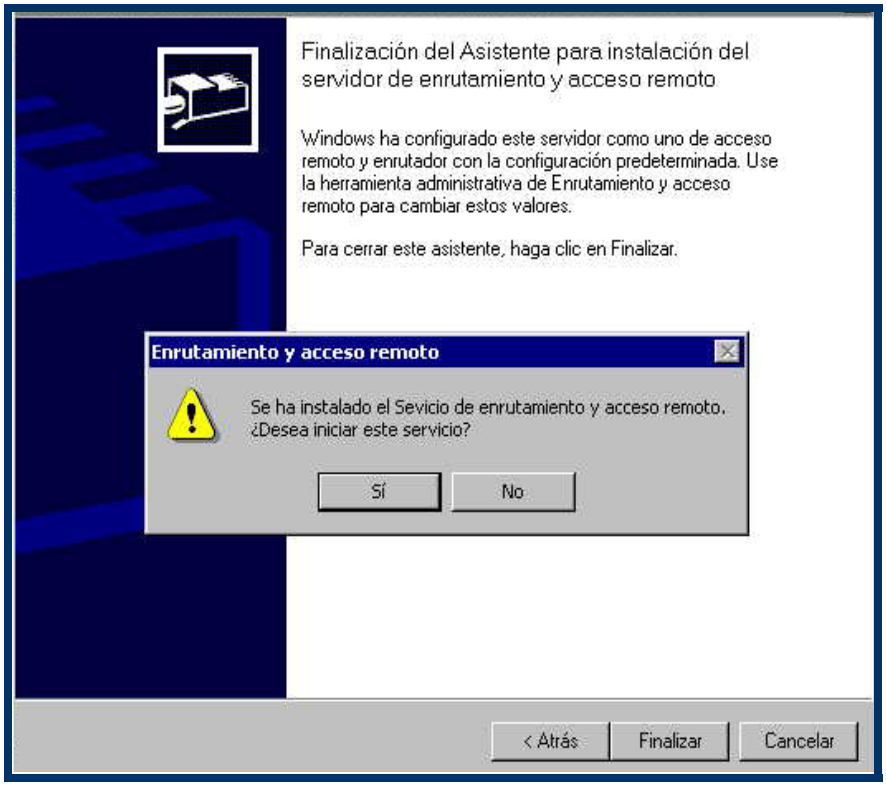


Ilustración V-9: Finalización del Asistente para instalación del servidor de enrutamiento y acceso remoto.

→ Una vez iniciado el servidor se procede a configurar los paramentos específicos para cada uno de sus componentes como se aprecia en la ilustración V-10.

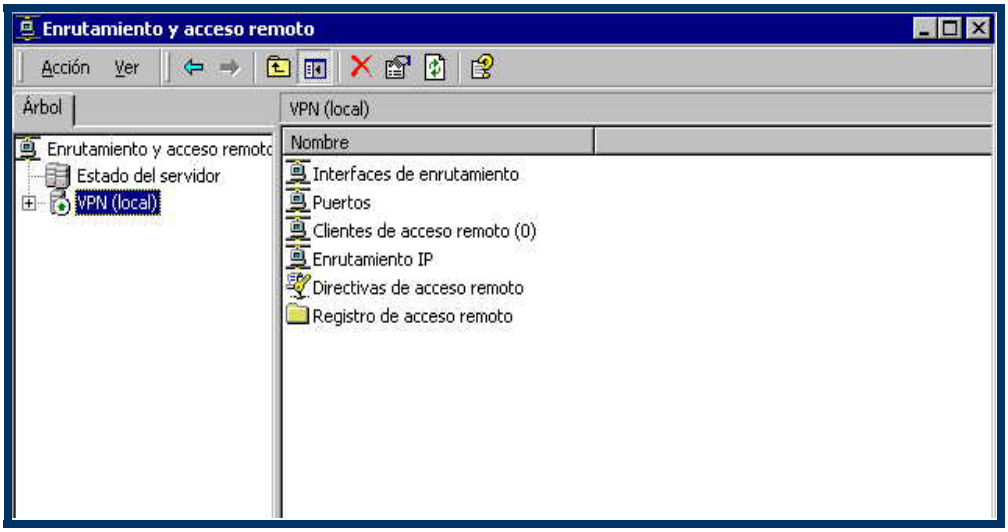


Ilustración V-10: Parámetros de Enrutamiento y Acceso Remoto.

→ Los únicos parámetros de configuración que se deben de modificar son los de la opción ***Puertos***, ***Directivas de acceso remoto*** y los de ***Registro de acceso remoto***, los demás se dejan con la configuración por defecto.

→ En la opción **Puertos** se configura el servidor VPN para utilizar 5 Túneles o puertos PPTP y 5 Túneles o puertos L2TP, como se muestra en la ilustración 69.

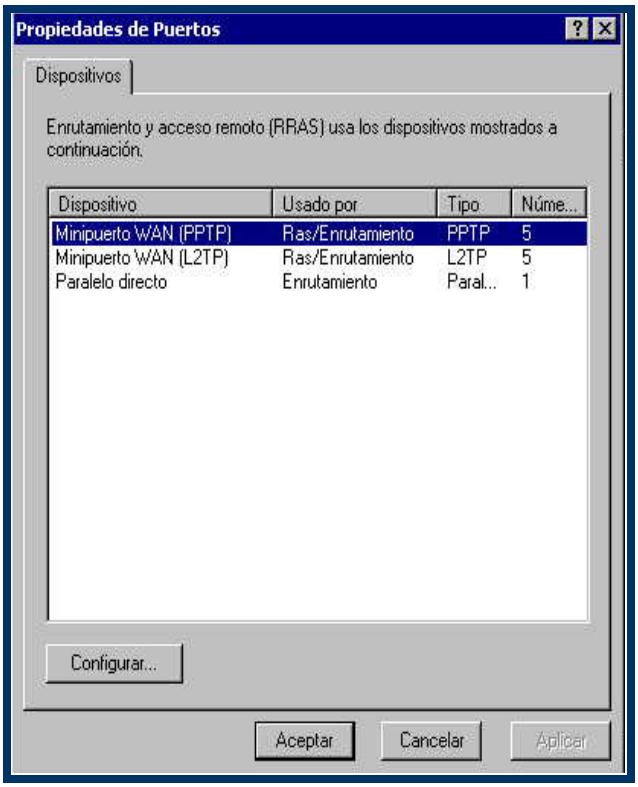


Ilustración V-11: Propiedades de Puertos.

→ Se debe de presionar el botón de Configurar para permitir que cada puerto (PPTP y L2TP) permitan conexiones de acceso remoto (De Entrada) y conexiones de enrutamiento de marcado a petición (De Entrada y Salida) como se muestra en la ilustración V-12.

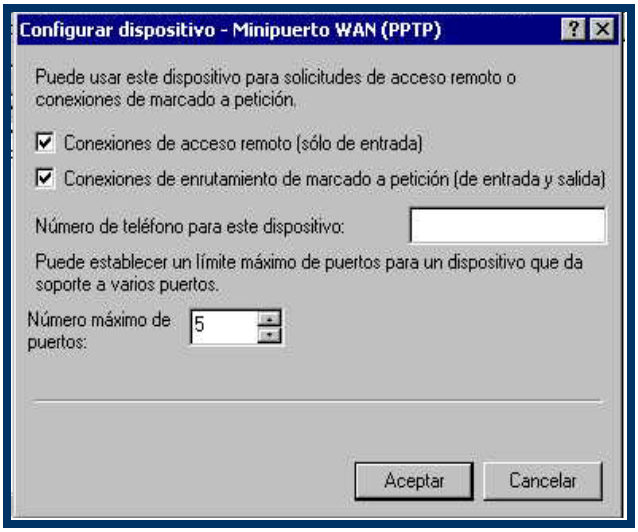


Ilustración V-12: Configuración de dispositivo - Minipuerto WAN (PPTP).

→ En la opción de Directivas de Acceso Remoto se deben de seleccionar las siguientes opciones, como se muestra en la ilustración V-13.

→ Condición: Permitir el acceso si está habilitado el permiso de acceso telefónico.

→ Permiso: Conceder permiso de acceso remoto.

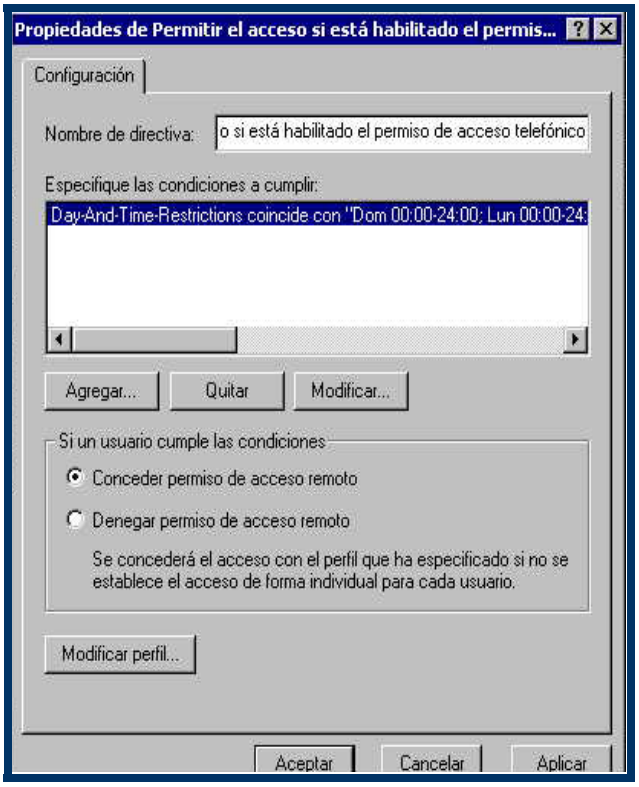


Ilustración V-13: Propiedades de acceso.

→ En Modificación de Perfiles se seleccionan las siguientes opciones:

- ❖ Ninguna restricción de marcado.
- ❖ Opción por defecto en la pestaña IP.
- ❖ Opción por defecto en la pestaña Mult.-Vínculo.
- ❖ Nivel de Cifrado Básico.
- ❖ Opción por defecto en la pestaña de Avanzado.
- ❖ En la opción de autenticación se debe de seleccionar el protocolo EAP, MS-CHAP y MS-CHAP v2.
- ❖ De igual forma se debe hacer clic en configurar para especificar el certificado que se utilizará para estos propósitos.

La ilustración V-14 muestra la configuración que se tiene que realizar para seleccionar los protocolos que habilitan el uso de certificados digitales como método de autenticación.

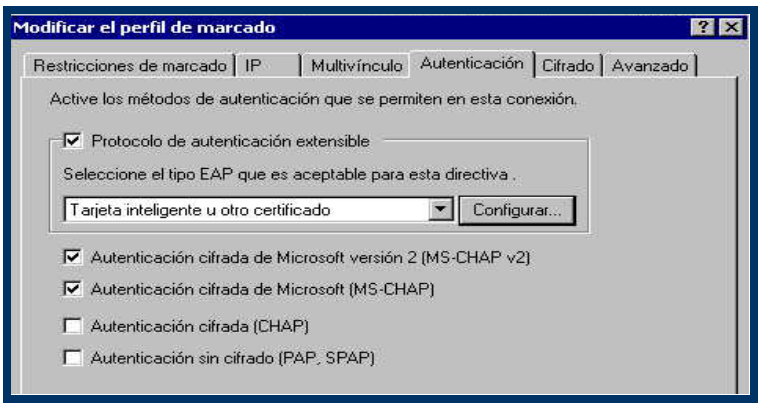


Ilustración V-14: Ventana para "Modificar el perfil de marcado".

La ilustración V-15 muestra el certificado que va a utilizar el servidor VPN para autenticación de clientes.

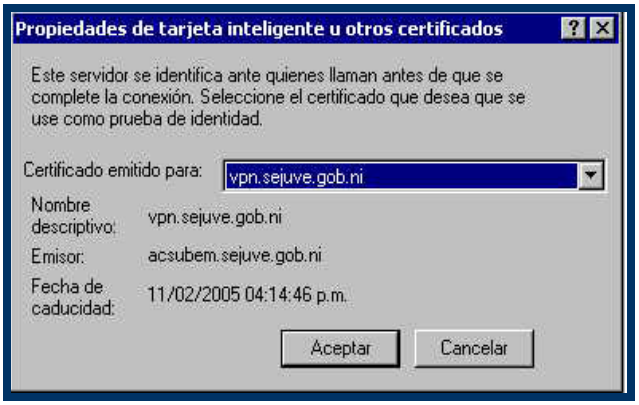


Ilustración V-15: Propiedades de tarjeta inteligente u otros certificados.

→ Los registros de acceso remoto de la actividad del servidor almacena en el archivo local C:\WINNT\system32\Logfiles como se muestra en la ilustración V-16.

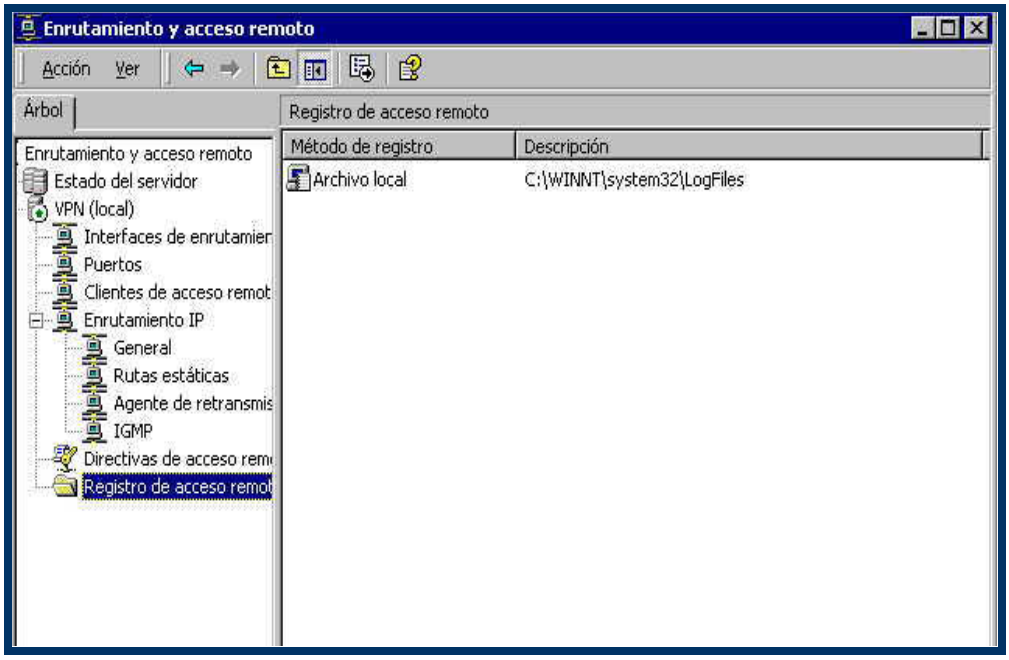
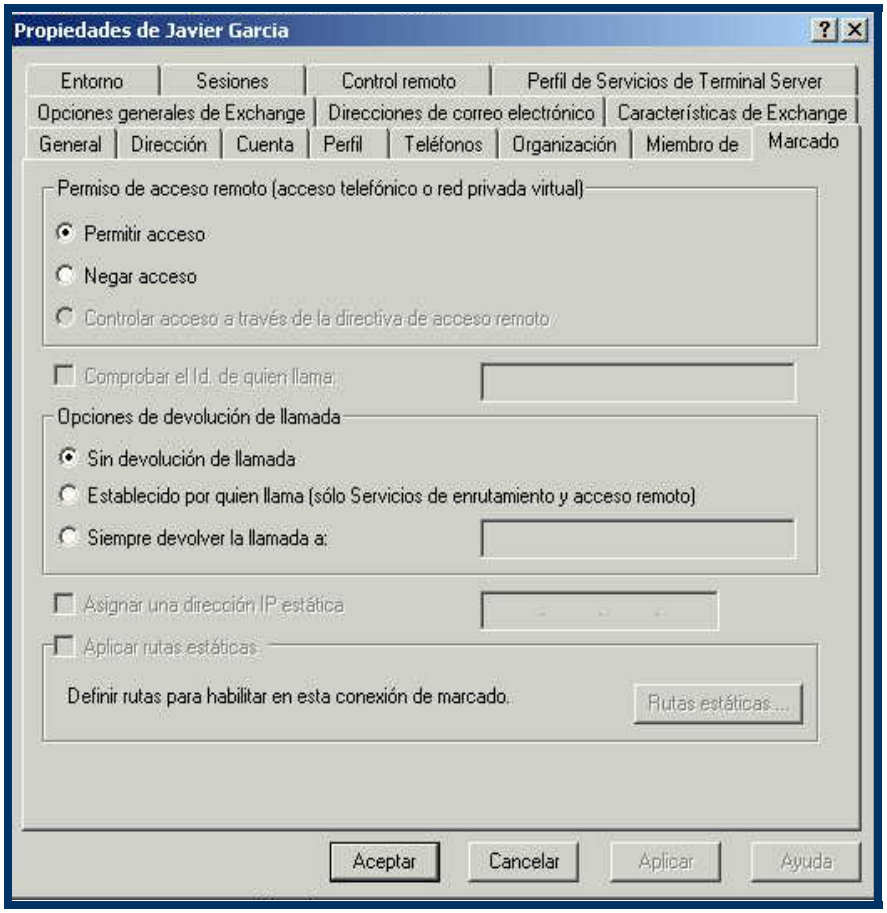


Ilustración V-16: Ventana de Enrutamiento y Acceso Remoto.

→ La última parte en la configuración del servidor VPN consiste en otorgar permiso de acceso remoto al o los usuarios de la VPN, en la pestaña **Marcado** de las propiedades de cada usuario en Active Directory del servidor principal como se muestra en la siguiente ilustración



3. Instalación del Cliente VPN

La instalación de los clientes VPN en este estudio se hará utilizando Windows XP utilizando L2TP como protocolo de túnel. El certificado para autenticación de clientes ya debe de estar instalado en el cliente antes de configurar la conexión.

La configuración de los clientes deben de realizarse después de la configuración del servidor VPN, y su uso tiene como condición principal disponer de una conexión a Internet, ya sea por teléfono o por una conexión dedicada.

a) El primer pasó para configurar el cliente VPN se realiza utilizando el módulo de conexiones de red en Panel de Control de Win XP como se muestra en la ilustración V-17.

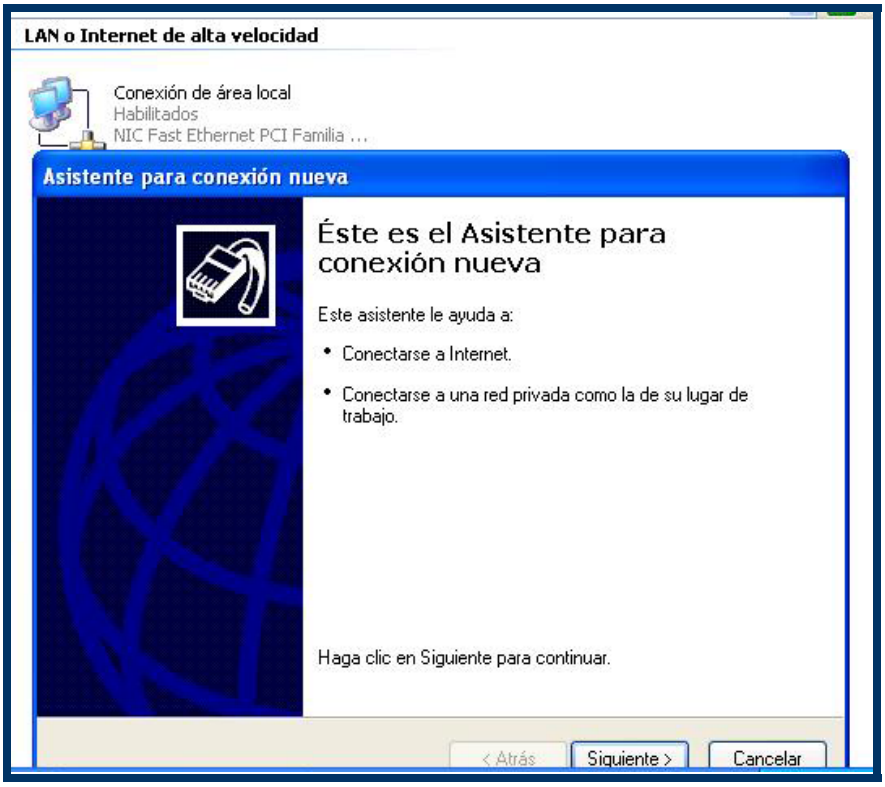


Ilustración V-17: Módulo de conexión de red en panel de control XP.

A través del módulo de conexiones de red se pueden configurar no sólo la conexión VPN, sino que también se utiliza para conectarse a Internet e incluso hasta conectar dos computadoras directamente a través del puerto serial.

b) Como siguiente paso se debe seleccionar Conectarse a la red de mi lugar de trabajo, ilustración V-18.

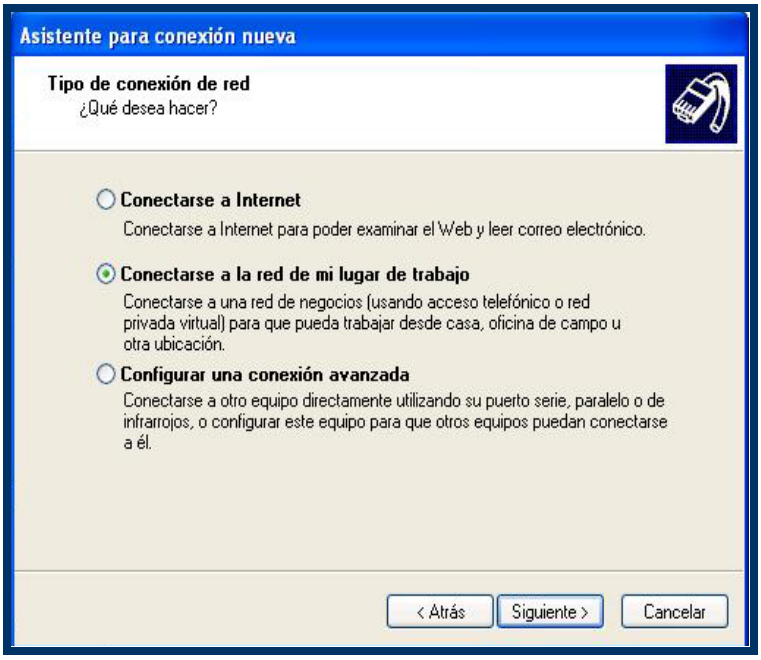


Ilustración V-18: Ventana de "Asistente para conexión nueva".

c) La opción seleccionada da paso a dos configuraciones específicas para acceso remoto, se debe seleccionar Conexión de red privada virtual ilustración V-19.

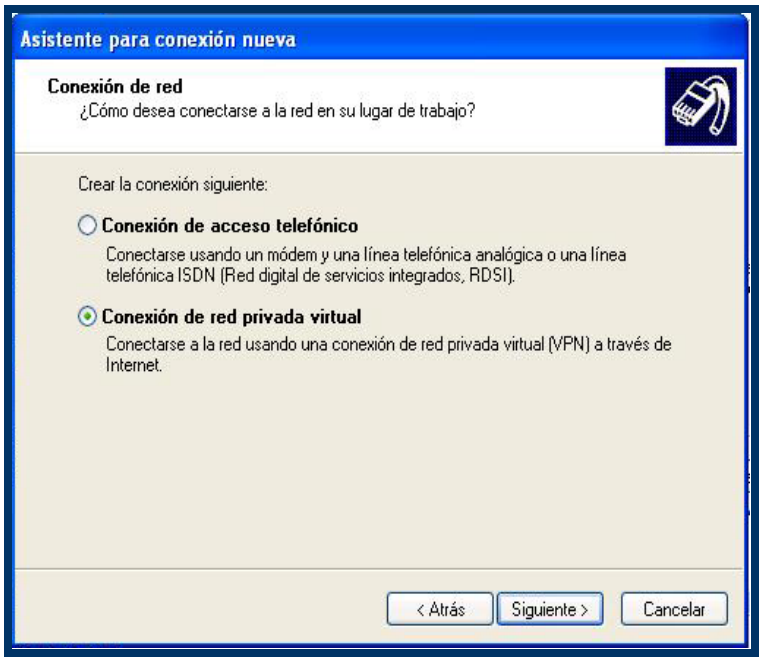


Ilustración V-19: Ventana de selección de "Conexión de red privada virtual".

A continuación se introduce un nombre identificativo para la nueva conexión que se está realizando.

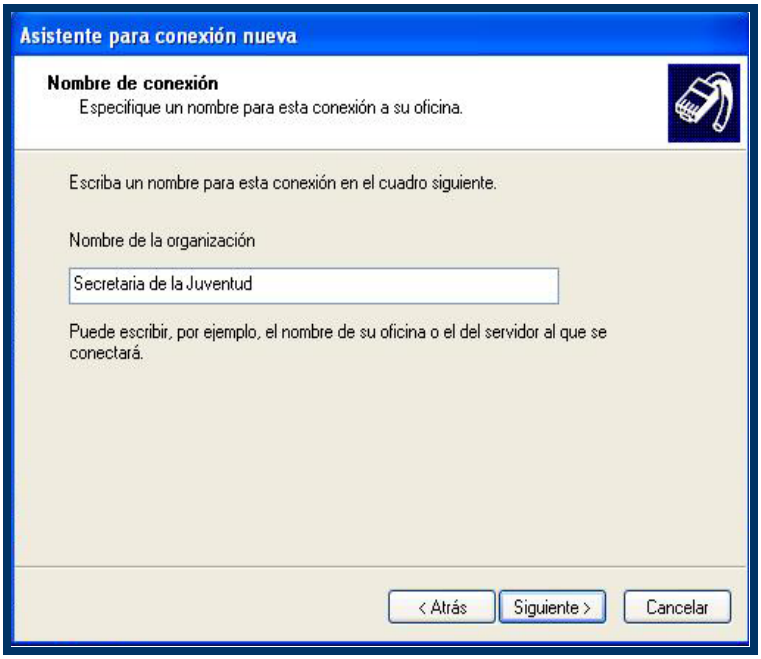


Ilustración V-20: Ventana de Asistente para conexión nueva.

d) Como siguiente paso se debe de introducir ya sea la dirección IP o el nombre del Servidor VPN, ilustración V-21.

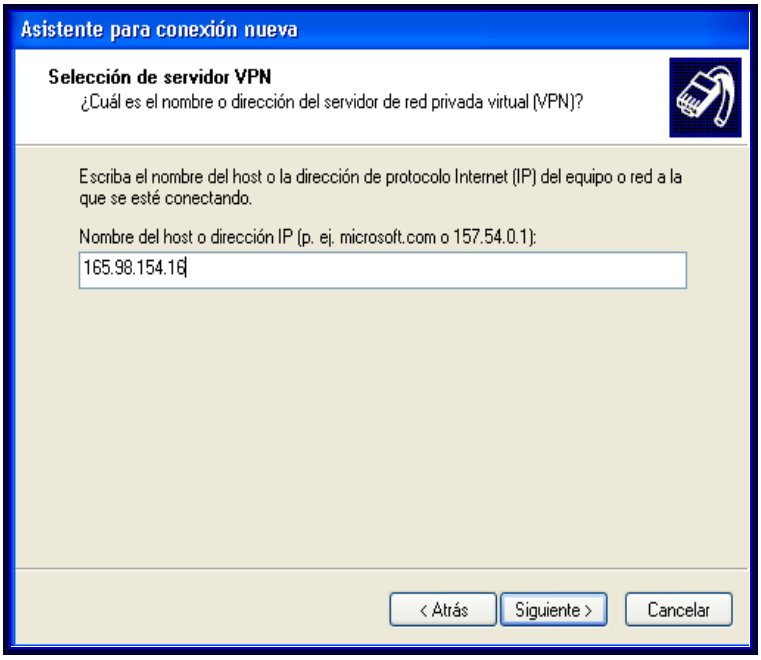


Ilustración V-21: Selección de servidor VPN.

e) El siguiente paso consiste en configurar los detalles propios para la conexión del cliente VPN.

En la pestaña de Opciones-> Opciones de Marcado se debe de elegir:

- ❖ Mostrar el progreso al conectar.
- ❖ Pedir el nombre, contraseña, certificado.

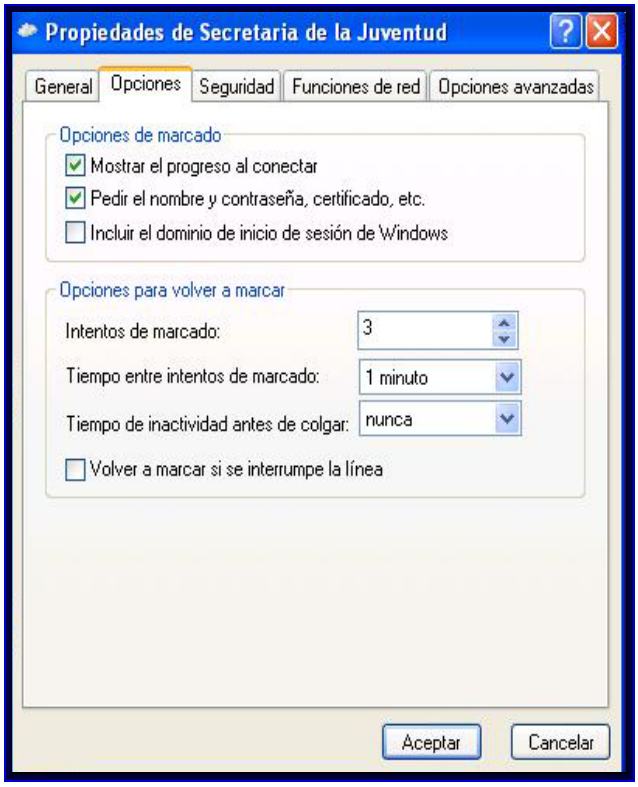


Ilustración V-22: Propiedades de la Secretaria de la Juventud.

En la pestaña de Seguridad se debe de seleccionar avanzado y luego seleccionar Usar el protocolo de autenticación extensible (EAP) como lo muestra la ilustración V-23.

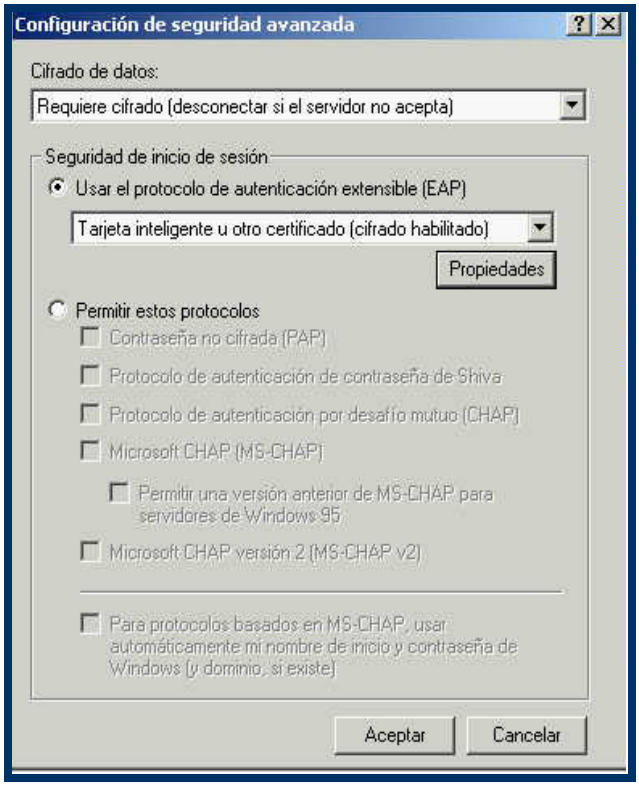


Ilustración V-23: Configuración de seguridad avanzada.

En la pestaña propiedades se selecciona toda la información concerniente al uso del certificado como se logra ver en la ilustración siguiente.

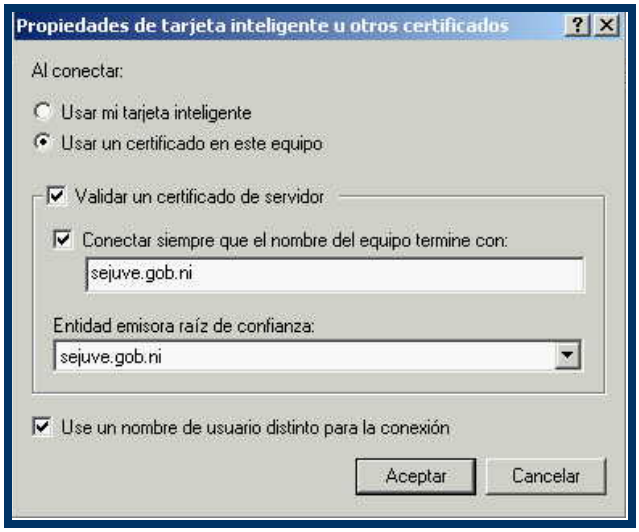


Ilustración V-24: Propiedades de tarjeta inteligente u otros certificados.

En la pestaña de Funciones de Red se debe de elegir el protocolo LPTP en el tipo de Túnel de la VPN para la utilización de certificados. Ilustración V-25

Ilustración V-25: Conexión privada virtual.

f) Verificar el certificado a utilizar

Una vez que se especifican todos estos detalles aparecerá la pantalla de la figura siguiente en la cual se especifica el certificado que se está utilizando para conectarse y permitirá al mismo tiempo utilizar otro nombre de usuario si así se desea. (Ilustración V-26)

Ilustración V-26: Verificación de la conexión privada virtual.

g) Conexión Realizada.

4. Filtros de Paquetes para la interfaz de Internet del Servidor VPN.

Debido a que la interfaz de Internet del servidor VPN tiene una dirección pública, a la que pueden acceder cualquier tipo de personas y provocar daños en la red interna, es necesario configurarla de tal manera que solo acepte específicamente el tráfico necesario para la conexión VPN.

Para realizar ésta tarea se debe entrar Enrutamiento IP -> General y presionar propiedades sobre la interfaz de Internet. (Ilustración V-27)

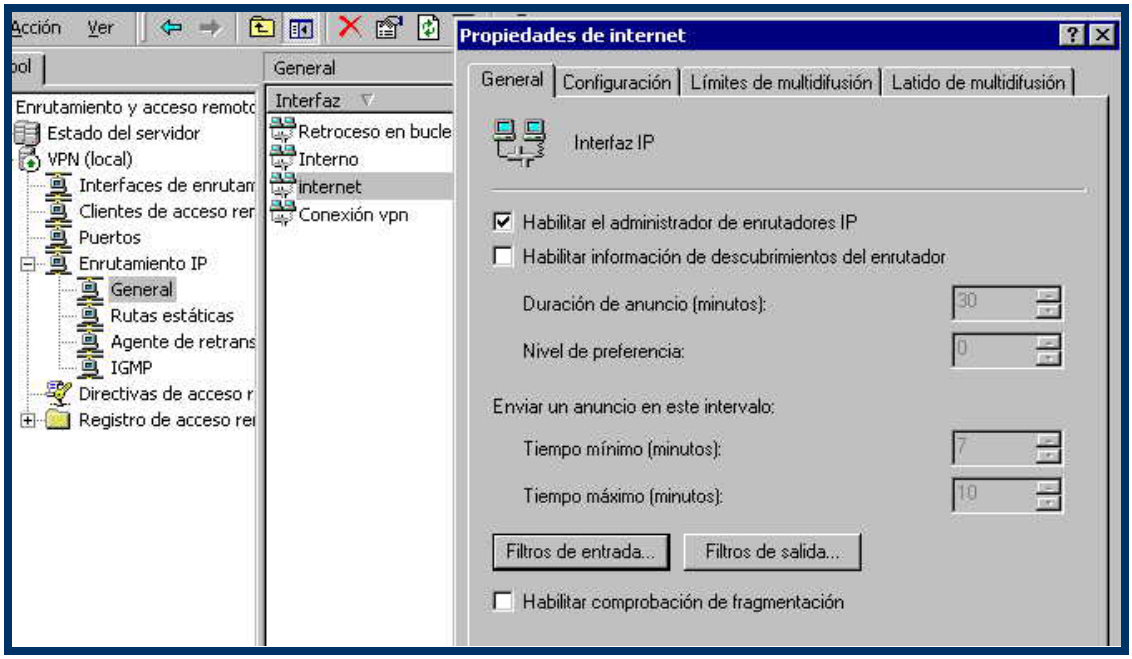


Ilustración V-27: Enrutamiento IP

Configurar los siguientes filtros de entrada con la acción de filtro descartar todos los paquetes excepto los que cumplen los siguientes criterios como lo muestran las siguientes ilustraciones:

+ Dirección IP destino: Dirección IP que posee la interfaz de Internet del servidor VPN.
+ Mascara de Subred: 255.255.255.255
+ Puerto UDP Destino: 500.

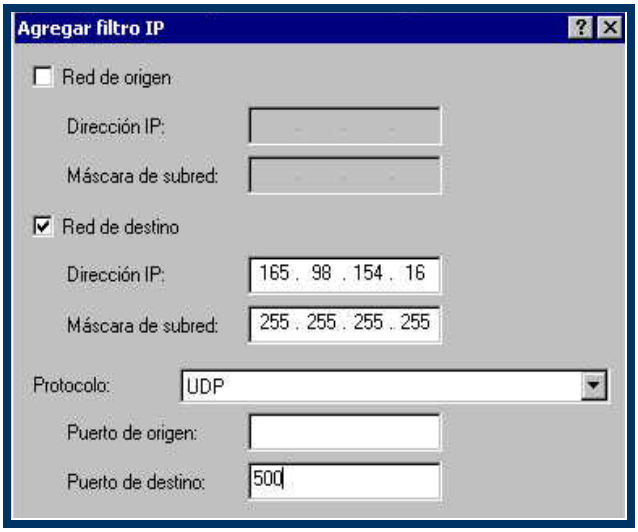
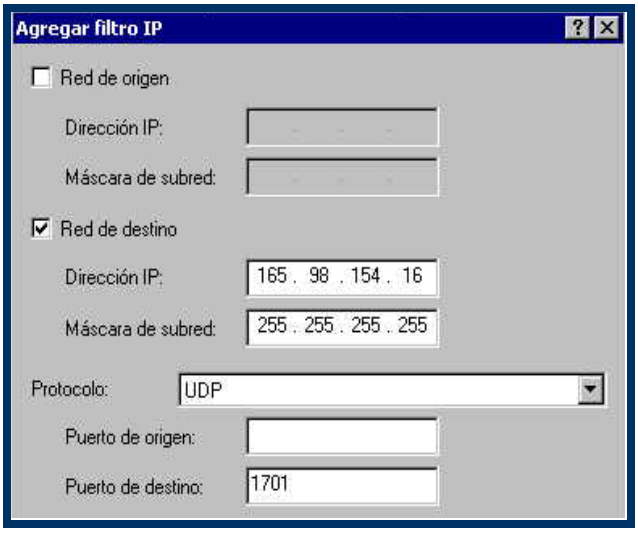


Ilustración V-28: Agregar un filtro IP

Este filtro permite el tráfico (IKE) hacia el servidor VPN.

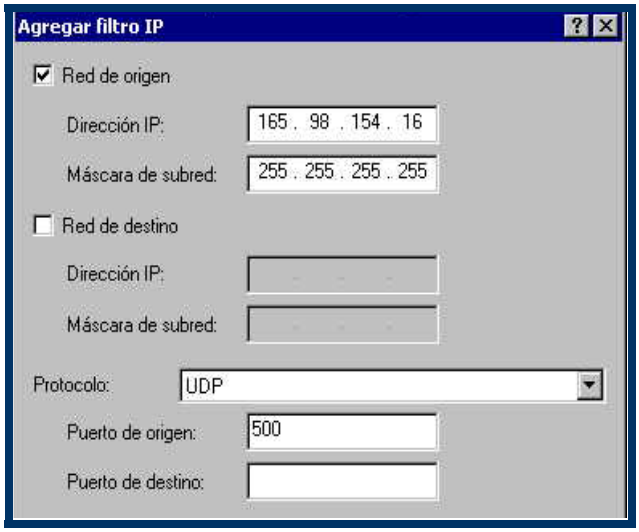
+ Dirección IP destino: Dirección IP que posee la interfaz de Internet del servidor VPN.
+ Mascara de Subred: 255.255.255.255
+ Puerto UDP Destino: 1701.



Este filtro permite el tráfico L2TP hacia el servidor VPN.

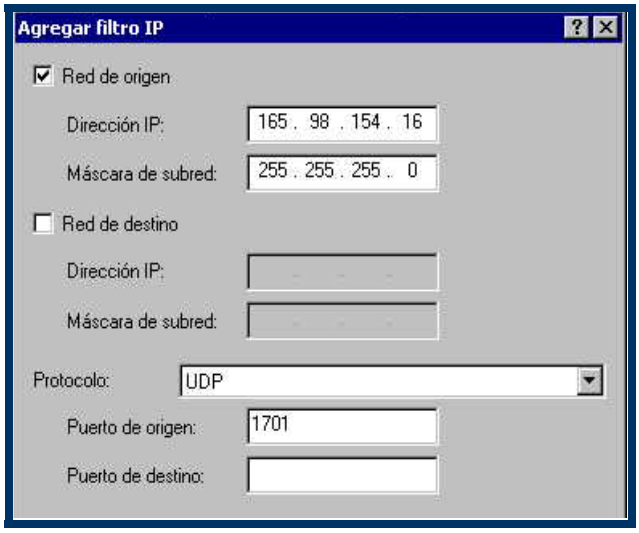
Configurar los siguientes filtros de salida con la acción de filtro descartar todos los paquetes excepto los que cumplen los siguientes criterios:

+ Dirección IP fuente: Dirección IP que posee la interfaz de Internet del servidor VPN.
+ Mascara de Subred: 255.255.255.255
+ Puerto UDP fuente: 500.



Este filtro permite el tráfico (IKE) desde el servidor VPN.

+ Dirección IP fuente: Dirección IP que posee la interfaz de Internet del servidor VPN.
+ Mascara de Subred: 255.255.255.255
+ Puerto UDP fuente: 1701.



Este filtro permite el tráfico L2TP desde el servidor VPN.

5. Enrutamiento del trafico VPN hacia la red interna.

Para lograr que los clientes VPN accedan a la red interna a través del servidor VPN es necesario configurarlo como un enrutador con una ruta estática que permita direccional el tráfico hacia la red interna.

La ruta estática se configura como se muestra la ilustración V-29

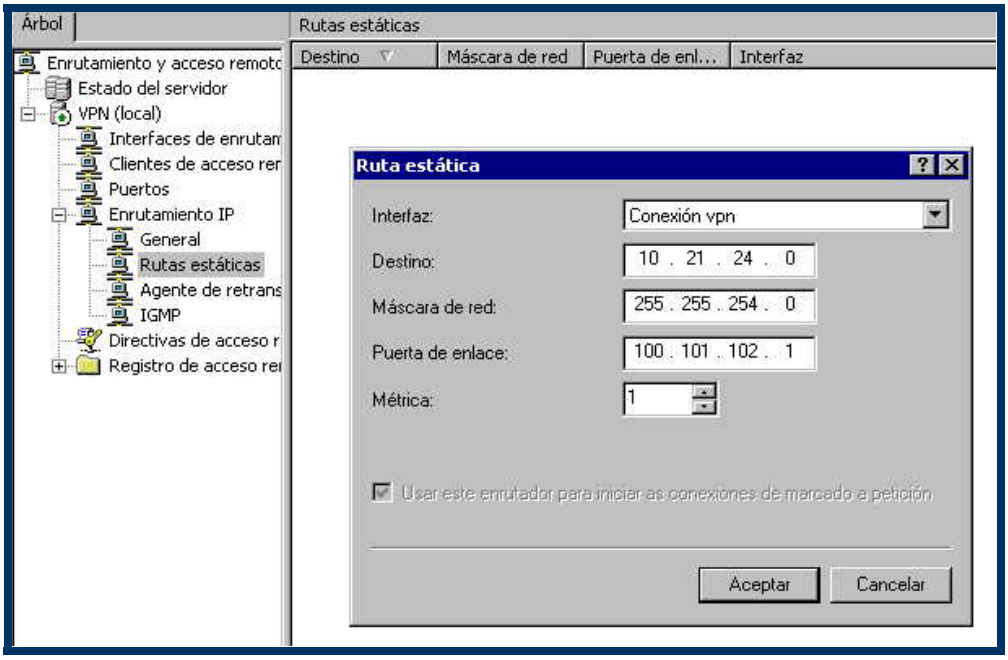


Ilustración V-29: Configuración de Ruta estática

6. Configuración del enrutador principal.

La configuración de este equipo está fuera del alcance de este estudio, además debido a que es el equipo principal de seguridad con que cuenta la SEJUVE, cualquier cambio inesperado en la configuración podría provocar que ésta quedará desprotegida y expuesta a ataques de personas malintencionadas, debido a eso solo se mostrara el procedimiento que se sigue para enrutador los datos hacia la red principal de la SEJUVE desde la interfaz del enrutador que esta conectada al Servidor VPN. Cabe aclarar que el procedimiento que se expone es exclusivo del software que el enrutador posee como lo es ASTARO LINUX SECURITY.

a. Definir la red VPN con los siguientes datos

Nombre: VPN_NET
IP: 100.101.102.0
Mascara de subred: 255.255.255.0.

b. Definir un grupo de seguridad que incluya las direcciones que se les otorgaran a los clientes VPN.

Nombre: Grupo_VPN
Direcciones:

Cliente1	100.101.102.3
Cleinte2	100.101.102.4
Cliente3	100.101.102.5
Cliente4	100.101.102.6
Cliente5	100.101.102.7
Cliente6	100.101.102.8
Cliente7	100.101.102.9
Cliente8	100.101.102.10
Cliente9	100.101.102.11
Cliente10	100.101.102.12

c. Mascara de Subred para todas 255.255.255.255

Definir y configurar la interfase del enrutador para el servidor VPN.

Nombre: VPN_internal
IP: 100.101.102.1
Mascara: 255.255.255.0
Gateway: Ninguno

d. Enrutamiento

Aquí se especifica el origen de los datos y el destino que deben seguir.

Red de Origen: VPN_NET
Interface destino: VPN_internal

e. Se debe especificar el tipo de paquetes y a quienes e le debe permitir pasar a través de esta interfaz:

From: Grupo_VPN.
To: Server (Nombre del Enrutador).
Service: Especificar los servicios permitidos para el funcionamiento de la VPN.
Action: Allow.

Al llegar a este punto se ha logrado completar las 6 principales etapas que se deben seguir para implementar una VPN con certificados digitales. Se debe de tener en cuenta que muchos de los parámetros de configuración que se utilizaron en este estudio son variables de acuerdo a las situaciones que se presenten y deben ser aplicadas según estudios previos realizados para cada institución en particular.

VI. CONCLUSIONES

CONCLUSIONES

1) La tecnología VPN es una tecnología económica, segura y flexible que permite automatizar el proceso de transferencia de información entre la SEJUVE y el SNIP.

2) La implementación de una VPN en una organización provoca un ahorro aproximado del 30 % en costos de comunicación en comparación con tecnologías inalámbricas dedicadas para la transmisión de información.

3) El uso de Internet como enlace de comunicación para una VPN permite que esta pueda ser utilizada a nivel mundial.

4) El protocolo de túnel L2TP/IPSEC provee el mayor grado de seguridad en la implementación de una VPN.

5) El protocolo L2TP/IPSEC permite la utilización de certificados digitales como método de autenticación.

6) La implementación de una VPN utilizando certificados digitales como método de autenticación evita la utilización de passwords los cuales se ven comprometidos con mayor facilidad.

7) La utilización de una infraestructura de clave pública permite la administración de certificados digitales utilizados para comprobar identidades.

8) Las tecnologías de Banda Ancha (Cable-MODEM, DSL, Wireless) son un medio barato de excelente velocidad para implementar una VPN.

VII. RECOMENDACIONES

RECOMENDACIONES

1) Utilizar la tecnología VPN con certificados digitales como solución de comunicación cuando dos empresas u organizaciones posean enlaces a Internet y quieran compartir y transmitir información entre si de manera segura, económica y flexible.

2) Se recomienda utilizar una conexión de Internet Inalámbrica de 512 Kbps para el enlace VPN de la SEJUVE, ya que por dificultades económicas, la implementación en este estudio se llevo a cabo utilizando un enlace por cable-MODEM de 256 Kbps.

3) Se recomienda llevar a cabo el proceso de configuración del enrutador principal descrito en este estudio para permitir que los usuarios del SNIP puedan acceder a la red interna de la SEJUVE, ya que por asuntos de seguridad no se llevó a cabo.

4) Se recomienda que se publiquen con cierta periodicidad las Listas de Revocación de Certificados de cada una de Autoridades Certificadoras, a fin de evitar que usuarios con certificados comprometidos o vencidos puedan acceder a información confidencial.

5) Se recomienda utilizar la PKI diseñada e implementada en este estudio no solo para emitir certificados de una VPN sino también para todas aquellas aplicaciones en las que es trascendental comprobar la identidad de las personas u equipos que interactúan entre si para compartir información.

VIII. ANEXOS

ANEXO A: INDICES DE ILUSTRACIONES Y TABLAS

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

ANEXO B: BIBLIOGRAFIA

BIBLIOGRAFIA

[TANENBAUMS91] Tanenbaum S, Andrew. Redes de Ordenadores (2da Edición) México Editorial Prentice Hall 1991

[FITZGERALD92] Fitzgerald, Jerry. Comunicación de Datos en los Negocios. (1era Edición) México Editorial Limusa S.A 1992

[SAMHERNADEZ94] Sampieri Hernández Roberto .Metodología de la Investigación Científica (2da Edición). México, DF. Editorial Publi-Mex 1994.

[BACAURBINA97] Baca Urbina Gabriel. Evaluación de Proyectos (3era edición) México Editorial Mc Graw Hill 1997.

[LEONCLARCK2000] Leon Clarck, David. Guía para el Administrador de Redes Privadas Virtuales(1era Edición) México Editorial McGrawHill 2000

[MICROSOFT2000] Microsoft On-Line Guía de Redes Privadas Virtuales 2000 Sitio Web http://www.microsoft.com/spanish/msn.

[CARBONELL99] Carbonell Castro Mildrey. Metodología para el diseño de una PKI. Tesis Universidad central " Martha Abreu " de las Villas.

[BROWN2000] Brown Steven. Implementación de Redes Privadas Virtuales (1era Edic) México Editorial McGrawHill 2000.

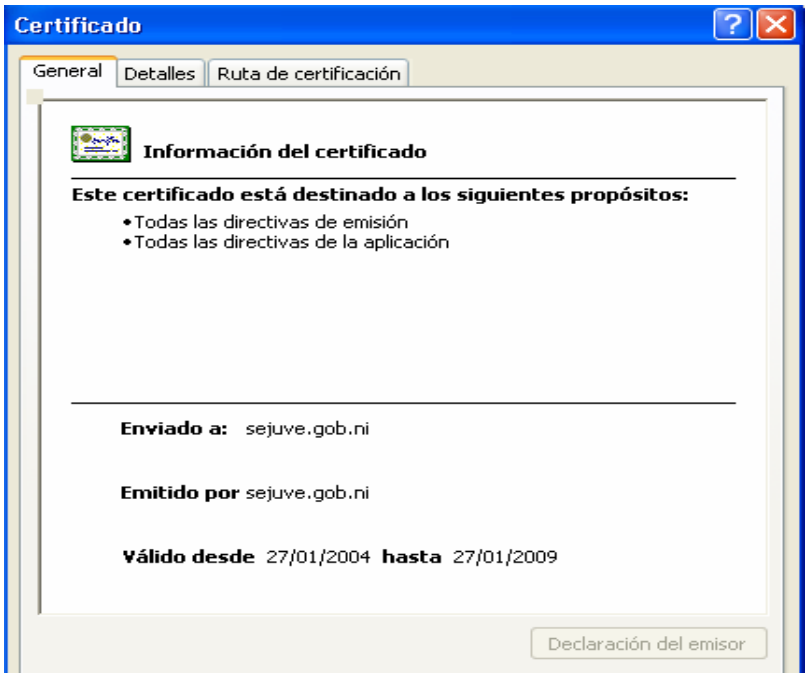
[MICROSOFT2000] Referencia Técnica a la Seguridad de Microsoft Windows 2000 Server. Microsoft Press. Capitulo 6 Criptografía e infraestructura de Clave Publica. Sitio Web: http://mspress.microsoft.com/prod/books/3873.html

[MICROSOFT2002] Microsoft Corporation . Deploying Remote Access VPNs with Windows 2000 Server. Microsoft Press July 2002.

ANEXO C: COTIZACIONES DE EQUIPOS Y CRONOGRAMA

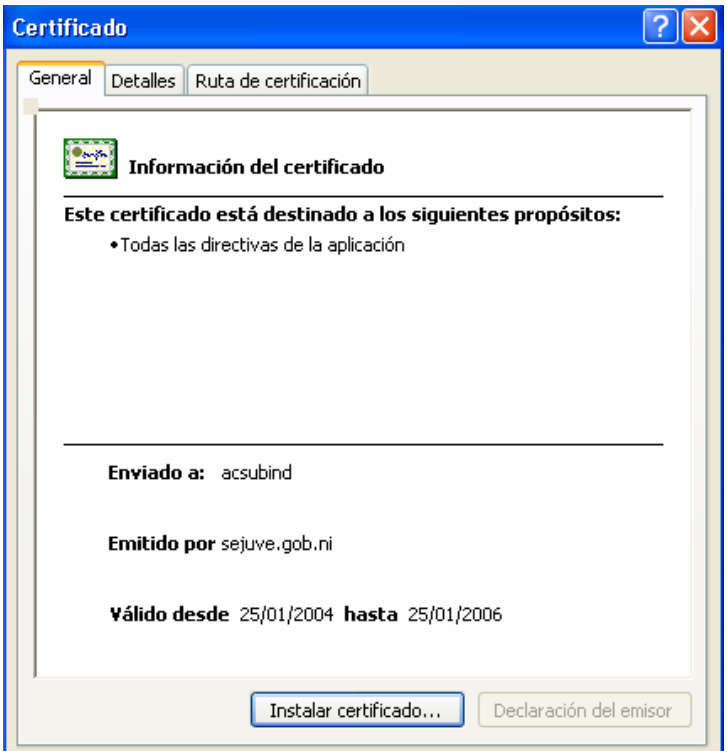
ANEXO D: CERTIFICADOS DIGITALES UTILIZADOS

CERTIFICADOS

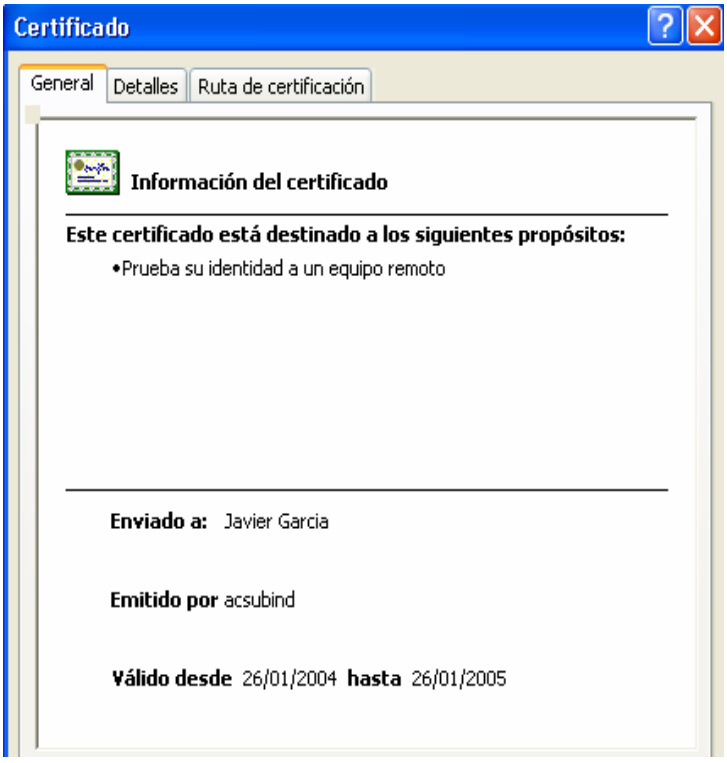


Certificado AC Raíz

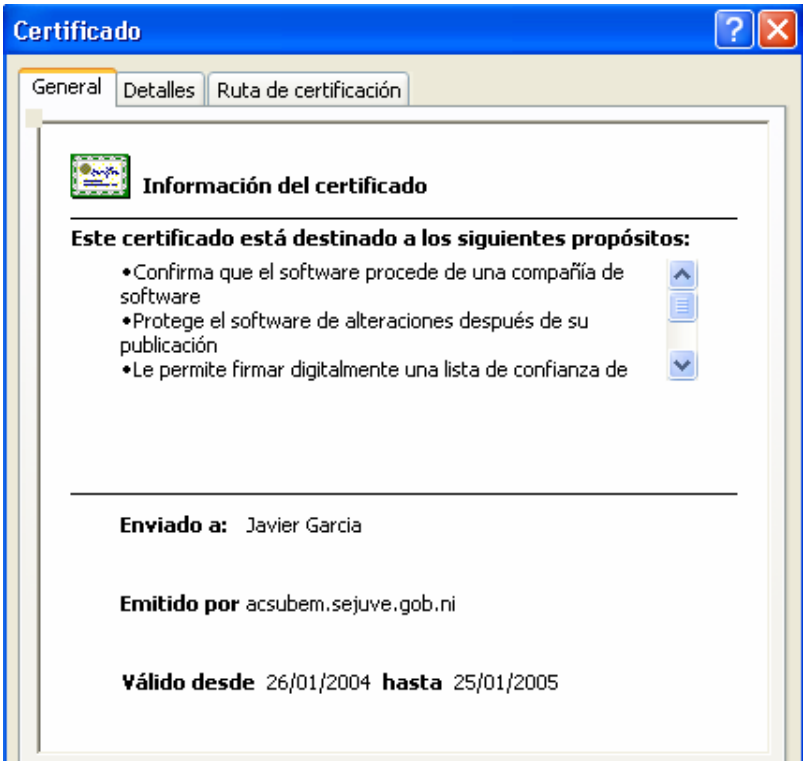
Certificado AC Subordinada Empresa



Certificado AC Subordinada Independiente



Certificado de Cliente o Usuario Externo



Certificado de Administrador

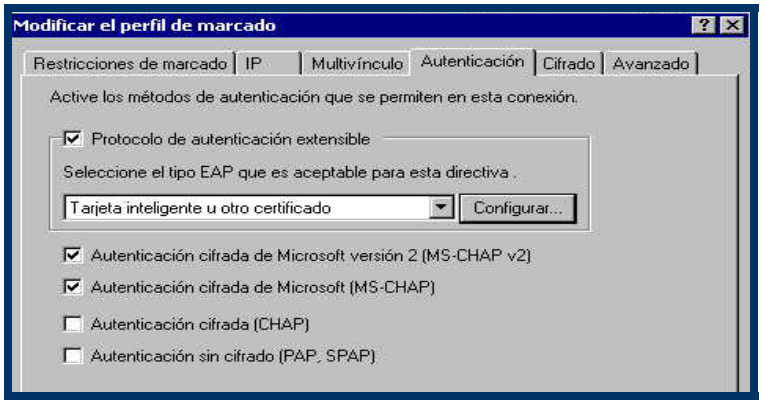
Certificado EFS para administrador

ANEXO E: VPN UTILIZANDO PPTP

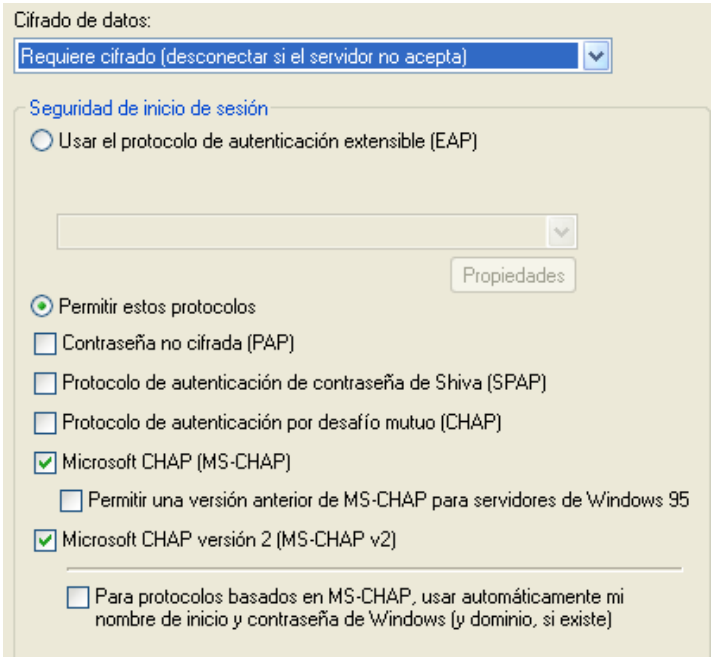
VPN UTILIZANDO PPTP

El procedimiento que se sigue para la implementación de una VPN utilizando PPTP es similar al que se sigue para L2TP teniendo como única diferencia el protocolo de autenticación que se utilice.

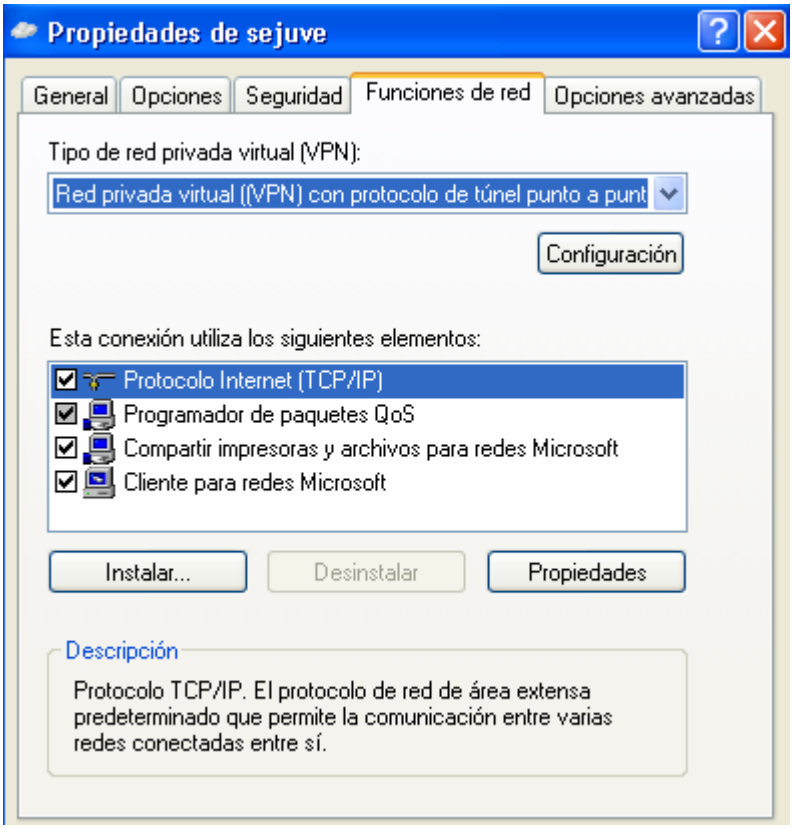
En el servidor VPN se debe utilizar únicamente los protocolos MS-CHAP v2 y MS-CHAP, como lo muestra la siguiente ilustración.



En los clientes VPN también se deben utilizar los protocolos MS-CHAP v2 y MS-CHAP como lo muestra la siguiente ilustración.



De igual forma se debe seleccionar VPN con protocolo PPTP en el tipo de red privada virtual en las funciones de red de las propiedades de la conexión VPN de los clientes como se muestra en la siguiente ilustración.



ANEXO F: DISEÑO METODOLOGICO

DISEÑO METODOLOGICO

a) Procedimientos para obtener información.

1. *Documental*

En este estudio, la mayor parte de la información se obtuvo a través de folletos y libros recopilados en Internet y en bibliotecas locales. La clasificación de la misma se llevó a cabo utilizando fichas bibliografías, cuyo contenido resumían las ideas principales de la información consultada.

2. *Entrevistas*

Para llevar a cabo este estudio se realizaron varias entrevistas a los directores de informática de las dos instituciones involucradas. Estas entrevistas facilitaron que los representantes de cada institución pudieran manifestar la problemática que enfrentaban las instituciones y al mismo tiempo explicar de manera breve la infraestructura actual con que se contaba. Para lograr esto se les hizo las siguientes preguntas

- ¿Como se realiza el proceso de transferencia de información entre las instituciones?
- ¿Poseen actualmente algún tipo de conexión a Internet?
- ¿Que tipo de datos se transmiten entre ambas instituciones?

3. *Observación y Experimentación*

Tanto la implementación de la VPN como la de la PKI, se llevaron a cabo a través de la experimentación y la observación de los resultados de los resultados que se iban obteniendo. La experimentación consistió en la realización de una serie de pruebas de configuraciones, las cuales fueron necesarias debido a que no se tenía ningún tipo de experiencia en el uso de las tecnologías utilizadas.

b) Enfoque del estudio

El enfoque que se plantea en este estudio es teórico-practico. Teórico, debido a que las tecnologías que se utilizan son relativamente nuevas y por lo tanto se requiere de una base consistente para poder entender su adecuado funcionamiento y Practico por que este estudio no se limitó a la fase de diseño, sino que fue mas allá de esta al realizarse diferentes comprobaciones en la implementación de estas tecnologías en ambas instituciones.

c) Lugar del estudio

La implementación de las tecnologías propuestas en este estudio se llevó a cabo en las instalaciones de cada una de las instituciones (SEJUVE y SNIP).

d) Herramientas de Procesamiento

Para procesar la información recopilada en este estudio se utilizaron principalmente las siguientes herramientas:

- Procesador de Palabras (WORD): Levantado y Diagramación de texto.
- Hoja de Calculo (EXCEL): Utilizado para el análisis cuantitativo de las soluciones propuestas.
- VISIO: Herramienta utilizada para la elaboración de los diseños de las soluciones propuestas.
- PROJECT: Herramienta utilizada para la calendarización y seguimiento de cada una de las etapas para la implementación de las tecnologías propuestas.

e) Herramientas y Procedimientos para el Desarrollo de Objetivos.

Para el análisis cuantitativo de las soluciones propuestas se hizo uso de un análisis costo beneficio, mediante el cual se pudo determinar la solución mas factible económicamente y los beneficios que esta conlleva.

La recomendación de la infraestructura de comunicación básica para una VPN se hizo en base en base a la teoría propia y la experiencia propia en el montaje de este tipo de tecnología.

Las comparaciones de tecnologías de túneles y de arquitecturas de VPN, se llevaron a cabo utilizando únicamente tablas comparativas basadas en la teoría recopilada.

Para el análisis, diseño e Implementación de la VPN y PKI, no se utilizó ninguna metodología de alguna empresa en particular, mas bien se definió una propia en base a los mejores elementos algunas de las metodologías encontradas en la documentación recopilada.

ANEXO G: GLOSARIO

GLOSARIO

Active Directory: En Microsoft Windows 2000 Server, Active Directory sustituye a la colección de funciones de directorios de Windows NT con una implementación integrada que incluye DNS, DHCP, LDAP y Kerberos.

Autenticación: Verificación de la identidad de un usuario o proceso de sistema.

Autoridad Certificadora (Certificate Authority, AC): El servicio que recibe y satisface las peticiones de certificado y las peticiones de revocación y que también puede administrar el proceso de registro (dirigido por cierta política) que realiza un usuario para conseguir un certificado.

Certificado: Una credencial usada para demostrar el origen, autenticidad y propósito de una clave pública a la entidad que tiene la clave privada correspondiente.

Controlador de dominio: Un servidor en un dominio que acepta accesos a cuentas e inicia su autenticación.

Controlador de dominio principal: En un dominio Windows NT, el servidor que autentica los accesos al dominio y mantiene la directiva de seguridad y la base de datos maestra de un dominio.

Cortafuego o Firewall: Un filtro protector para accesos al sistema y mensajes. Una organización conectada directamente al Internet lo utiliza para evitar accesos no autorizados a su red.

Dirección IP: Un número de cuatro partes separadas por puntos que identifica unívocamente a una maquina en Internet. Cada máquina de Internet tiene una dirección IP única; si una máquina no tiene una dirección IP, en realidad no esta en Internet.

Dominio: En Windows 2000, un grupo de equipos que comparte una directiva de seguridad y una base de datos de cuentas de usuario.

Enrutador o Encaminador: Una computadora (o paquete software) de propósito especial que manipula la conexión entre dos o más redes. Los enrutadores examinan las direcciones de destino de los paquetes que pasan a su través y deciden que camino usar para enviarlos.

Host: Cualquier dispositivo de la red que utilice TCP/IP. Un host es también un equipo en Internet en el que se puede iniciar una sesión.

Kerberos: Un sistema de seguridad basado en identidad que autentica a los usuarios en el inicio de sesión. Funciona mediante la asignación de una clave única, llamada vale, a cada usuario que inicia sesión en la red.

Lista de revocación de certificados (CRL): Una lista firmada digitalmente (publicada por una autoridad de certificado) de certificados que ya no son validos.

Protocolo de acceso ligero a directorios, (LDAP): Un protocolo que se usa para acceder a un servicio de directorio. LDAP es una versión simplificada de Protocolo de acceso a Directorios (DAP), que se utiliza para obtener acceso a directorios X.500. LDAP es el protocolo de acceso principal de Active Directory.

Protocolo de configuración dinámica de host (DHCP): Un protocolo de TCP/IP utilizado para asignar direcciones IP y configurar TCP/IP automáticamente en los clientes de red.

Protocolo de Internet (IP): El protocolo de la capa de trabajo de Internet utilizado como base de Internet. IP permite el enrutamiento de la información de una red a otra dividida en paquetes y posteriormente reconstruida cuando éstos alcanzan su destino.

Protocolo de Túnel Punto a Punto (PPTP): Un protocolo que permite conexiones de enrutador a enrutador y de host a red a través de una línea telefónica.

Servicio de Usuario de acceso telefónico de autenticación remota (RADIUS): Un sistema de autenticación de seguridad utilizado por muchos proveedores de servicios de Internet. Un usuario se conecta con el ISP e introduce un nombre de usuario y contraseña. Esta información es verificada por un servidor RADIUS, que autoriza a continuación el acceso al sistema ISP.

Servidor: Un equipo que proporciona un servicio a otros sistemas en una red. Un servidor de archivos, por ejemplo, proporciona archivos a las maquinas cliente.

Servidor Miembro: Un equipo que ejecuta Windows 2000 Server o Windows NT Server que no es un controlador de dominio. Los Servidores miembro pueden dedicarse a administrar archivos, servicios de impresión u otras funciones.

Servidor de nombres DNS: Servidor que contienen información sobre las partes de la base de datos del Sistema de nombres de dominio (DNS). Estos servidores hacen disponibles los nombres de los equipos para consultas sobre resolución de nombres a través de Internet.

X. 500: Un estándar para un servicio de directorio establecido por la Unión internacional de telecomunicaciones (ITU). Este estándar define el modelo de información utilizado en el servicio de directorio.